Secure Short-Packet Multihop Communications with Friendly Jammers

Toan-Van Nguyen*, Thai-Hoc Vu†, Daniel Benevides da Costa‡, and Duy H. N. Nguyen*
* Dept. of Electrical and Computer Engineering, San Diego State University, San Diego, CA 92182 USA
† School of Electrical Engineering, University of Ulsan, 44610 Republic of Korea
‡ Dept. of Electrical Engineering, King Fahd University of Petroleum & Minerals, Dhahran 31261, Saudi Arabia
Emails: *vannguyentoan@gmail.com, †vuthaihoc1995@gmail.com, ‡danielbcosta@ieee.org, *duy.nguyen@sdsu.edu

***Abstract*—In this paper, we propose a best node and friendly jammer (bN-fJ) scheme for secure short-packet multi-hop communications in Internet-of-Things (IoT) networks. Under imperfect channel state information (CSI) conditions, the best IoT node is chosen for data transmission and a friendly jammer is chosen later to confuse the received signals at a multi-antenna eavesdropper. Approximate and asymptotic closed-form expressions for the secrecy throughput of the bN-fJ scheme are obtained, offering valuable insights into the system designs. Numerical results show that the proposed bN-fJ scheme achieves much better performance than benchmarking schemes, especially with 1 more bit/channel use and 9.4 dB enhancement in communication reliability measure. Moreover, under imperfect CSI and large antennas at the eavesdropper, the secrecy throughput and communication reliability of the system can be improved by employing the proposed node selection, e.g., a 12.5 dB improvement at 10 antennas at Eve and the imperfect CSI of 0.8. Finally, the secrecy throughput is presented as a concave curve for the number of hops and blocklengths, which enables us to identify the optimal hops and blocklength for secure multi-hop short-packet transmissions.**

***Index Terms*—IoT networks, PHY security, short-packet multi-hop communications, and URLLCs.**

I. Introduction

Short-packet communication (SPC) has recently gained significant momentum thanks to its latency-sensitive applications, such as reliable remote action with robots in factory automation or coordination among vehicles [1]. SPCs primarily emphasize the pursuit of ultra-reliable communications while maintaining a low block-error rate (BLER) [2], for example, the reliability of SPCs in IoT systems has reached 99.999 percent with a latency of 1 ms [3]. Compared to long-packet communications, SPC can help to minimize the end-to-end (e2e) transmission latency because of using a small number of channel uses. However, it comes with the cost of coding gain reduction, which brings challenges in reliability transmission and security. Moreover, the incorporation of short-packet communications in 5G and Internet-of-Things (IoT) networks establishes novel communication paradigms linked to theoretical principles. These paradigms challenge conventional analysis frameworks relying on Shannon's capacity, rendering them no longer valid. In particular, within the constraints of SPC, capacity evaluation requires handling an intricate function involving blocklength, BLER, and transmit power, posing computational challenges for performance analysis.

Physical-layer security (PLS) in IoT systems with SPCs has recently received much attention, stemming from its advantage of not necessitating additional resources for secure ultra-reliable low-latency communication applications [4]–[6]. By exploiting the intrinsic physical properties and randomness of wireless channels, such as fading, noise, or smart signaling, to degrade the received signal qualities of malicious users, PLS can realize keyless secure transmission via signal design and adaptive transmission protocols [7]. Encryption and key-exchange procedures in upper layers are quite complex for IoT devices with a shortage of power, storage, and computing capabilities. However, using short packets results in a reduction of secrecy capacity since blocklengths are no longer sufficiently large to reach the maximal transmission rate, which is typically considered in conventional physical security to ensure both reliability and security [4]. Hence, employing short-packets in IoT systems might increase their vulnerability to security attacks [4]. In [8], the authors explored single-hop communication systems, wherein an access point not only transmitted short packets to an actuator but also generated artificial-noise-aided signals to confound a multi-antenna eavesdropper. The study in [9] derived a closed-form expression for the secrecy throughput for full-duplex SPCs in multiple-input multiple-output systems. Additionally, asymptotic analysis was conducted for infinite blocklength, high transmit power, and large antenna number of antennas at the access point. Short packet suspicious communications were studied in [10] to evaluate the success probability maximization problem.

Thus far, most secure short-packet communication studies only focused on single-hop, except for [11], while secure multi-hop transmission in IoT systems that deal with a powerful Eve equipped with diversity combining technology has not been well addressed. Particularly, the salient aspect of imperfect channel state information (CSI) in finite blocklength systems is not thoroughly investigated, especially when transmitting packets over multiple hops. In this context, the predominant challenges involve the integral of the Q-function, especially when addressing the average secrecy throughput analysis. This motivation prompts us to investigate the per-

This work was supported by the U.S. National Science Foundation under grants ECCS-2146436 and CCF-2322190.

formance of secure short-packet multi-hop communications in IoT systems with imperfect CSI and multiple antennas at the eavesdropper as well as to propose an efficient, yet low-complexity jamming scheme. Our recent work [11] has analyzed the secrecy BLER and throughput of multi-hop transmission but considered non-colluding Eves, while a powerful Eve with multiple antennas and using a diversity combining technique for eavesdropping on short-packets over multi-hop legitimate transmission has not yet been discovered.

In this paper, we further extend our previous findings on secure multi-hop SPCs [11] by considering a powerful Eve equipping with multiple antennas and using the maximum-ratio combining (MRC) technique, the contributions of this paper can be summarized as follows:

- We propose a best node and friendly jammer (bN-fJ) scheme to enhance the security and communication reliability of multi-hop short-packet multi-hop transmissions in the presence of a multi-antenna Eve using MRC.
- We derive new closed-form expressions for the average secrecy throughput of the proposed bN-fJ scheme, accompanied by concise asymptotic analyses for extreme values of blocklength and transmit power. The accuracy of the developed analysis is affirmed through Monte-Carlo simulations.
- We show through numerical results that the secrecy throughput and communication reliability improvement of the proposed bN-fJ scheme over the baseline ones, such as the best IoT node selection and without jammer (bN-woJ), the random node and best jammer (rN-bJ) selection, and the random node and friendly jammer (rN-fJ) selection schemes under different information leakage and imperfect CSI levels.
- Several further insights can be drawn from the developed analyses as follows: choosing a random IoT node is more advantageous than choosing the best one, especially in scenarios with severely imperfect CSIs. The secrecy throughput is presented as a concave curve for the number of hops and blocklengths, which enables us to identify the optimal hop and blocklength for secure short-packet multi-hop transmissions. Furthermore, adjusting an appropriate number of IoT nodes in intermediate clusters can improve the system secrecy throughput. Finally, deploying more IoT devices in the perfect CSI will be more effective than the imperfect CSI one in improving communication reliability when Eve uses large antennas.

The remainder of this paper is organized as follows. Section II presents the system model, including the proposed node selection strategy and the eavesdropping scenario. In Section III, the analysis of secrecy throughput is detailed, emphasizing both approximation and asymptotic expressions for the average secrecy throughput. Section IV shows numerical results to validate the analytical findings presented in Section III. The paper concludes in Section V.

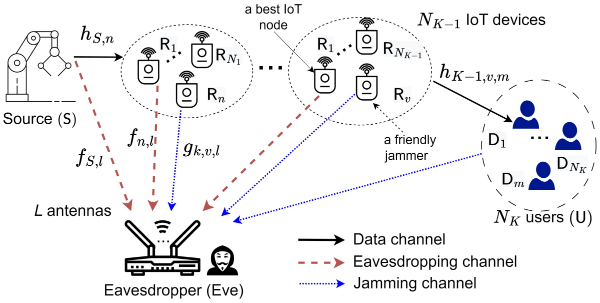


Fig. 1: The proposed secure transmissions for factory automation applications.

II. System Model

We consider a secure short-packet multi-hop communication system within an automation factory, as depicted in Fig. 1. In this setup, multiple IoT devices, organized into $K-1$ clusters, collaborate to perform multi-hop ultra-reliable low-latency communications (URLLCs) from a robot source (S) to a set of user destinations $\mathcal{D} = \{\mathsf{D}_m\}_{m=1}^{M}$. We denote by $\mathsf{R}_{k,n}$ the n-th IoT device in the k-th cluster, employing a randomize-and-forward protocol for packet transmission across multiple hops [12]. Simultaneously, an eavesdropper with L antennas endeavors to eavesdrop on the exchanged messages among IoT nodes. During each hop transmission, one or more friendly jammers will be selected among available IoT nodes to confuse the received signals at the eavesdropper. It is assumed that the source and all IoT nodes are single-antenna devices operating in half-duplex mode.

Let us represent the channel coefficients as $h_{k,i,n}$, $f_{k-1,l}$, and $g_{k,j,l}$, corresponding to the links from $\mathsf{R}_{k-1,i}$ to $\mathsf{R}_{k,n}$, from $\mathsf{R}_{k-1,i}$ to l antenna at E, and from $\mathsf{R}_{k,j}$ to l antenna at E, respectively. Here, $\mathsf{R}_{0,i}$ and $\mathsf{R}_{K,m}$ are seen as S and D_m, respectively. We assume all channels follow frequency-flat fading, which accounts for the effects of both small-scale fading and large-scale path loss. Therefore, each channel coefficient, denoted as $\tilde{z} \in \{h_{k,i,n}, f_{k-1,l}, g_{k,j,l}\}$, can be presented as $z = \sqrt{H_z}\tilde{z}$, where $\tilde{z}$ is the small-scale Rayleigh fading and H_z is the large-scale path loss. The channel gain $|z|^2$ follows an exponential distribution with parameter λ_z. The large-scale path loss can be modeled as $H_z = \frac{\mathcal{L}}{(d_{\mathsf{UV}}/d_0)^{\eta}}$ denotes the large-scale path loss, taking into account the Euclidean distance between $\mathsf{U} \in \{\mathsf{S}, \mathsf{R}_{k-1,i}, \mathsf{R}_{k,j}\}$ and $\mathsf{V} \in \{\mathsf{R}_{k,n}, \mathsf{D}_m, \mathsf{E}\}$ d_{UV}, the path loss exponent η, the reference distance d_0, and the measured pathloss at d_0 $\mathcal{L}$.

In this system, secure packet transmission is evenly distributed across K orthogonal time slots during K hops. Each time slot, indicated by the total number of channel uses (CUs) c_T and the duration of each CU T, is calculated as $c_T T/K$. In real-world scenarios, attaining perfect CSI of data channels proves challenging due to feedback delays in IoT nodes within dynamic environments. Let denote $\widehat{h}_{k,i,n}$ as the estimated version of $h_{k,i,n}$, we have $\widehat{h}_{k,i,n} = \rho h_{k,i,n} + \sqrt{1-\rho^2}\xi_k$, where ξ_k is a circular symmetric complex Gaussian random variable with zero mean and the same variance as $h_{k,i,n}$, and $\rho \in [0,1]$ denotes the correlation coefficient between the envelopes of $h_{k,i,n}$ and $\widehat{h}_{k,i,n}$. The bN-fJ scheme is proposed to enhance secrecy performance while reducing processing complexity for energy-constrained IoT nodes. Within each cluster, IoT devices collaborate to select an IoT node providing the highest channel gain from the transmitter for packet transmission. Subsequently, a friendly jammer is randomly selected from the remaining ones, tasked with generating jamming signals to disrupt the signals intercepted by the Eve while ensuring that all legitimate IoT nodes are not harmed [12]. Denoting by R_{k-1,i^*} the selected node at cluster $k-1$, the criterion to select the best node at cluster k can be presented as

$$\mathsf{R}_{k,n^*} = \arg \max_{n=1,\ldots,N_k} |\widehat{h}_{k,i^*,n}|^2. \tag{1}$$

The instantaneous SNR at the selected node R_{k,n^*} under imperfect CSI can be expressed as

$$\gamma_{k,n^*} = \max_{n=1,\ldots,N_k} \frac{P_{k-1}}{\sigma_k^2} |\widehat{h}_{k,v^*,n}|^2, \tag{2}$$

where P_{k-1} is the transmit power of R_{k-1,i^*} and σ_k^2 denotes Gaussian noise variance. A friendly jammer at cluster k is then randomly selected to produce jamming signals, aiming to hinder the eavesdropper interception. The received signal at the Eve can be presented as

$$y_{\mathsf{E},k} = \sqrt{P_{k-1}} f_{k-1,l} + \sqrt{P_k} g_{v,l} + n_{\mathsf{E}}, \tag{3}$$

where $g_{v,l}$ denotes the channel coefficient from a friendly jammer $\mathsf{R}_{k,v}$ to the Eve and n_{E} is the additive white Gaussian noise. The Eve with L antennas deploys the MRC technique to combine its received signals. Thus, the instantaneous SNR at hop k wiretapped by the Eve with jamming strategy can be expressed as

$$\gamma_{\mathsf{E},k} = \sum_{l=1}^{L} \frac{P_{k-1}|f_{k-1,l}|^2}{P_k|g_{v,l}|^2 + \sigma_{\mathsf{E}}^2}, \tag{4}$$

where σ_{E}^2 denotes the Gaussian noise variance. For ease of notation, we denote $\psi_k = P_{k-1}/\sigma_k^2$ and $\psi_{\mathsf{E},k} = P_{k-1}/\sigma_{\mathsf{E}}^2$.

III. Secrecy Throughput Analysis

In an SPC system with a quasi-static fading wiretap channel, a positive secrecy rate exists when the SNR of the legitimate channel is larger than that of Eve's channel. It is considered a finite blocklength transmission at hop k, the maximum instantaneous secrecy rate r_k for a given blocklength $c_D > 100$, a decoding error probability (or the secrecy BLER) ϵ_k, and an information leakage δ_k over a wiretap channel can be expressed as [13]

$$r_k = \begin{cases} C_k - \sqrt{\frac{S_k}{c_D}} Q^{-1}(\epsilon_k) - \sqrt{\frac{S_E}{c_D}} Q^{-1}(\delta_k), & \gamma_{k,n^*} > \gamma_{\mathsf{E},k}, \\ 0, & \gamma_{i,n^*} < \gamma_{\mathsf{E},k}. \end{cases} \tag{5}$$

where m denotes the number of bits encoded into a packet being transmitted from $\mathsf{R}_{k-1,i}$ to $\mathsf{R}_{k,n}$, $c_D = c_T/K$, $C_k = \log_2(1+\gamma_{k,n^*}) - \log_2(1+\gamma_{\mathsf{E},k})$ represents the secrecy capacity of the eavesdropping system under short block-length constraint, $Q^{-1}(.)$ denotes the inverse Gaussian Q-function. Moreover, the channel dispersion of legitimate and eavesdropping channels can be presented, respectively, as $S_k = (\log_2 e)^2 \big(1 - \frac{1}{(1+\gamma_{k,n^*})^2}\big)$ and $S_E = (\log_2 e)^2 \big(1 - \frac{1}{(1+\gamma_{\mathsf{E},k})^2}\big)$.

It can be seen in (5), when $\gamma_{k,n^*} < \gamma_{\mathsf{E},k}$, the secrecy BLER $\epsilon_k = 1$. When $\gamma_{k,n^*} \geq \gamma_{\mathsf{E},k}$, the secrecy BLER at hop k can be derived as

$$\epsilon_k = Q\Big(\sqrt{\frac{c_D}{S_k}}\Big[\log_2 \frac{1+\gamma_k}{1+\gamma_{\mathsf{E},k}} - \sqrt{\frac{c_D}{S_E}} Q^{-1}(\delta_k) - \frac{m}{c_D}\Big]\Big). \tag{6}$$

The secrecy throughput under finite blocklength regimes at hop k is calculated as

$$\tau_k = r_k(1 - \mathbb{E}\{\epsilon_k\}), \tag{7}$$

where $\mathbb{E}\{\epsilon_k\}$ represents the average secrecy BLER at hop k and $\mathbb{E}\{\cdot\}$ stands for the expectation operator.

Theorem 1. *Under finite blocklength conditions, the end-to-end (e2e) secrecy throughput achieved by the bN-fJ scheme can be expressed as*

$$\tau_{e2e} = r_k \prod_{k=1}^{K} (\mathcal{T}_{1,k} - \mathcal{T}_{2,k}), \tag{8}$$

$$\mathcal{T}_{1,k} = \sum_{n=0}^{N_k-1} \binom{N_k-1}{n} \frac{(-1)^n N_k}{n+1} \exp\Big(\frac{1-\omega_k}{\psi_k \Omega_k}\Big), \tag{9}$$

$$\mathcal{T}_{2,k} = \widehat{\sum} \exp\Big(\frac{1-\omega_k}{\psi_k \Omega_k} + \beta_k \Upsilon_k\Big) \frac{N_k \Gamma(1+q) \beta_k^{l-i+1} \omega_k \mathcal{U}}{(\lambda_{E,k}\psi_{\mathsf{E},k})^{l-q} \psi_k \Omega_k}, \tag{10}$$

where

$$\mathcal{U} = \begin{cases} (\Upsilon_k)^{q-i} \Gamma(i-q, \beta_k \Upsilon_k), & i > q, \\ \frac{(\Upsilon_k)^{q-i}}{(q-i)!} \Big[\sum_{d=1}^{q-i} \frac{\Gamma(d)\exp(-\beta_k \Upsilon_k)}{(-\Upsilon_k \beta_k)^d} + E_1(\beta_k \Upsilon_k) \Big], & i \leq q, \end{cases} \tag{11}$$

$$\Omega_k \triangleq \frac{(1+n-n\rho^2)\lambda_k}{(n+1)}, \Upsilon_k \triangleq \frac{\lambda_{E,k}^{-1}}{\psi_{E,k}} + \frac{\omega_k}{\psi_k \Omega_k}, \beta_k = \frac{\lambda_{E,k}}{\rho \lambda_{E,J_k}} \tag{12}$$

$$\widehat{\sum} = \sum_{n=0}^{N_k-1} \sum_{l=0}^{L-1} \sum_{q=0}^{l} \sum_{i=0}^{l} \binom{l}{q} \binom{l}{i} \binom{N_k-1}{n} \frac{(-1)^{l+n-i}}{l!(n+1)}, \tag{13}$$

and $E_1(.)$ is the exponential integral function [14, Eq. (1)].

Remark 1: When N_k in (9) and (10) increases, the e2e secrecy throughput in (8) significantly improves. When the imperfect CSI level is large, i.e., a small value of ρ, Ω_k is large, making $\mathcal{T}_{2,k}$ in (10) become smaller and the secrecy throughput reduces, causing a low throughput for multi-hop packet transmissions. Furthermore, ψ_k is inversely proportional to $\mathcal{T}_{2,k}$, thus a large transmit power at each IoT device, i.e., when ψ_k rises, the e2e secrecy throughput also increases.

Theorem 2. *At high SNR regimes, the asymptotic expression for the e2e secrecy throughput of bN-fJ scheme can be expressed as*

$$\tau_{\mathtt{asym}}^{\mathtt{SNR}} \overset{\psi \to \infty}{\approx} r_k - \sum_{k=1}^{K} \widehat{\sum} \frac{r_k N_k \Gamma(1+q) \omega_k \beta_k^{l-i+1}}{\psi_k \Omega_k (\lambda_{E,k} \psi_{E,k})^{l-q}} \mathcal{U}, \tag{14}$$

where $\psi \in \{\psi_k, \psi_{E,k}\}$.

From (14), the asymptotic secrecy throughput reduces when the number of hops K increases. However, when ψ in the denominator in the second term of (14) increases, $\tau_{\mathtt{asym}}^{\mathtt{SNR}}$ will be reduced. Furthermore, the end-to-end secrecy throughput in (14) exhibits an inverse relationship with the CSI conditions, denoted as Ω_k, and a direct proportionality with the number of IoT devices.

Theorem 3. *In the finite blocklength regimes, the asymptotic expression for the e2e secrecy throughput of bN-fJ scheme can be expressed as*

$$\tau_{\mathtt{asym}}^{c_D} \overset{c_D \to \infty}{\approx} r_k \prod_{k=1}^{K} \left[1 - \widehat{\sum} \frac{N_k \Gamma(1+q) \exp(\beta_k \Theta_k) \mathcal{U}}{\beta_k^{i-l-1} \psi_k \Omega_k (\lambda_{E,k} \psi_{E,k})^{l-q}} \right], \quad (15)$$

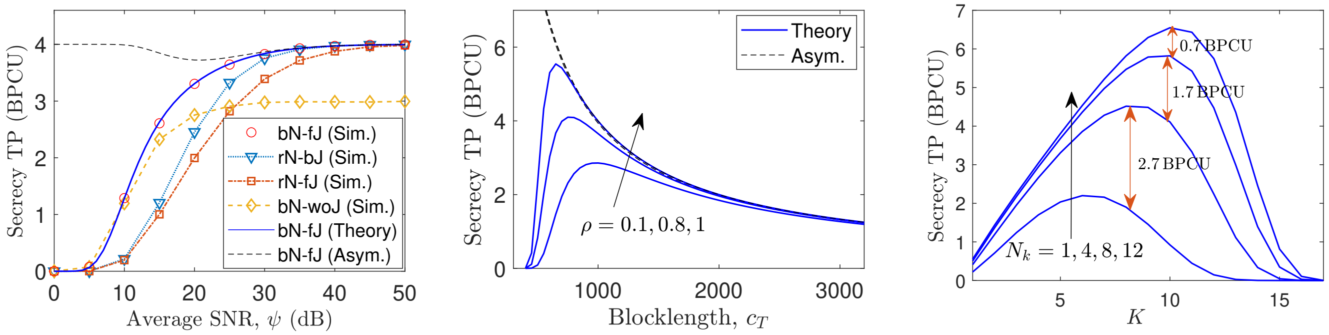
where $\Theta_k = 1/(\lambda_{E,k}\psi_{E,k}) + 1/(\psi_k \Omega_k)$.

In the finite blocklength regimes, we have $\lim_{c_D \not\to +\infty} \omega_k = 1$. By substituting $\omega_k = 1$ into (8), $\tau_{\mathtt{asym}}^{c_D}$ can be obtained as (15). *Remark 2:* In the finite blocklength regimes, the e2e secrecy throughput remains constant irrespective of the blocklength. As shown in (15), the effect of imperfect CSI is less significant in infinite blocklength regimes with moderate ψ_k. The reason is that the imperfect CSI coefficient associated with Ω_k will have less influence on the secrecy throughput when it is in a product of $\psi_k \Omega_k$, therefore, ψ_k will have more influence on the secrecy throughput.

IV. Numerical Results

In this section, we provide numerical results for evaluating system secrecy performance. To validate our designed approach, Monte Carlo simulations are employed to assess the average secrecy throughput and secrecy BLER. On the Euclidean plane, the robot S, IoT devices R_k, the user U, and eavesdroppers E are situated at coordinates $(0,0)$, $(k/K, 0)$, $(25, 0)$, and $(30, 20)$, respectively. We set the parameters as follows: $d_0 = 1$ m, $\sigma^{\mathtt{PL}} = -30$ dB, $\mathtt{PL} = 3.5$, average SNR $\psi_k = \psi_D = \psi_E = \psi$, and normalized noise variance $\sigma^2 = 1$. Unless explicitly stated otherwise, the remaining simulation parameters are configured as $K = 5$, $N = 4$, $L = 4$, imperfect CSI parameter $\rho = 0.8$, information leakage $\delta_k = 0.1$, number of bits $m = 800$, and total channel uses $c_T = 1000$. Fig. 2(a) shows the significant secrecy throughput improvement of the bN-fJ scheme over the rN-bJ, rN-fJ, and bN-woJ ones. As observed, the bN-fJ scheme improves 1 bit per channel use (BPCU) of secrecy throughput on average at moderate SNRs compared to the rN-bJ one, which underscores the effectiveness of choosing the best IoT nodes with the highest channel gain for secure short-packet multi-hop transmission. Furthermore, the bN-fJ scheme has 1 BPCU of secrecy throughput higher than the bN-woJ one at high SNRs, which indicates the potency of deploying a friendly jammer to degrade Eve's channels. In addition, the high average SNR increases the probability of successfully receiving packets, which makes all schemes achieve their largest secrecy throughput at high SNRs. Importantly, the simulated results of the bN-fJ scheme closely match the theoretical ones while the asymptotic results tightly align with analysis derivations at high SNRs. This consistency demonstrates the accuracy of our derivations as presented in Theorems 1 and 2. In Figs. 2(b) and 2(c), the secrecy throughput is depicted as a function of both the number of hops and blocklengths. By configuring a constant number of information bits for transmission across different blocklengths, the secrecy throughput initially increases, reaching its peak before gradually declining in infinite blocklength regimes. This phenomenon encompasses a trade-off between the fixed coding rate r_k and the secrecy throughput in (8), wherein a constant quantity of bits transmitted over longer blocklengths reduces the secrecy throughput. Furthermore, the figure also shows that the secrecy throughput of the bN-fJ scheme under perfect CSI can improve up to 3 BPCU compared to its counterpart with severe imperfect CSI, i.e., $\rho = 0.1$, at the optimal blocklengh. Moreover, the asymptotic secrecy throughput of perfect CSI and imperfect CSI at large blocklenghs is almost the same, which indicates a tiny effect of imperfect CSI on the secrecy throughput of the system under large blocklengh conditions, which also aligns with insights in Remark 2. In Fig. 2(c), as the number of hops K rises, the secrecy throughput experiences an initial increase, reaching its peak because of the decreasing impact of pathloss via transmitting over multiple hops. However, with continued increases in K, the secrecy throughput eventually reduces, reaching zero. This decline is due to a substantial increase in error probability with an extensive number of transmission hops, as indicated in (6). Moreover, increasing the appropriate number of IoT devices can improve significantly the secrecy throughput, for example, when N_k increases from 1 to 4, the secrecy throughput can be increased up to 2.7 BPCU. However, by increasing an additional 4 IoT nodes, the secrecy throughput improves only 1.7 BPCU. Therefore, deploying the appropriate IoT nodes in each cluster can achieve the best trade-off between implementation cost and secrecy throughput.

Fig. 3(a) illustrates the effect of imperfect CSI on the proposed bN-fJ and rN-bJ schemes with different transmission hops. For high levels of imperfect CSI, i.e., when ρ is small, the rN-bJ scheme demonstrates greater efficiency compared to the bN-fJ scheme. This is due to the presence of severely outdated CSI with high levels of imperfection leading to an inaccurate selection of the best node in the bN-fJ scheme. Conversely, with low imperfection in CSI, i.e., when ρ is large, the strategy of selecting the best node becomes more efficient, resulting in an increase in secrecy throughput for the bN-fJ scheme. For instance, there is a notable increase of 2.6 BPCU with 10 hops at $\rho = 0.8$. Furthermore, there exist levels of imperfect CSI at which the bN-fJ scheme outperforms the rN-bJ scheme. Fig. 3(b) provides an insight into the security-reliability trade-off for the proposed bN-fJ scheme. The average e2e secrecy BLER can be obtained from (8) as $\varepsilon_{e2e} = 1 - \tau_{e2e}/r_k$. As observed, the average secrecy BLER of the bN-fJ scheme decreases with an increase in the information leakage δ_k. A higher probability of information leakage, represented by a larger δ_k, indicates a reduced correlation between confidential messages and the eavesdropper's observation, thereby lowering the secrecy BLER. In addition, the proposed rN-fJ scheme has the highest communication reliability among other ones under different information leakage levels. For example, the bN-fJ scheme offers at least 9.4 dB of reliability better than the rN-bJ one, i.e., improving from $\varepsilon_{e2e} = 5.4 \times 10^{-2}$ to $\varepsilon_{e2e} = 2.1 \times 10^{-2}$. Fig. 3(c) shows the effects of the number of antennas at the Eve on the average secrecy BLER with perfect and imperfect CSI conditions.

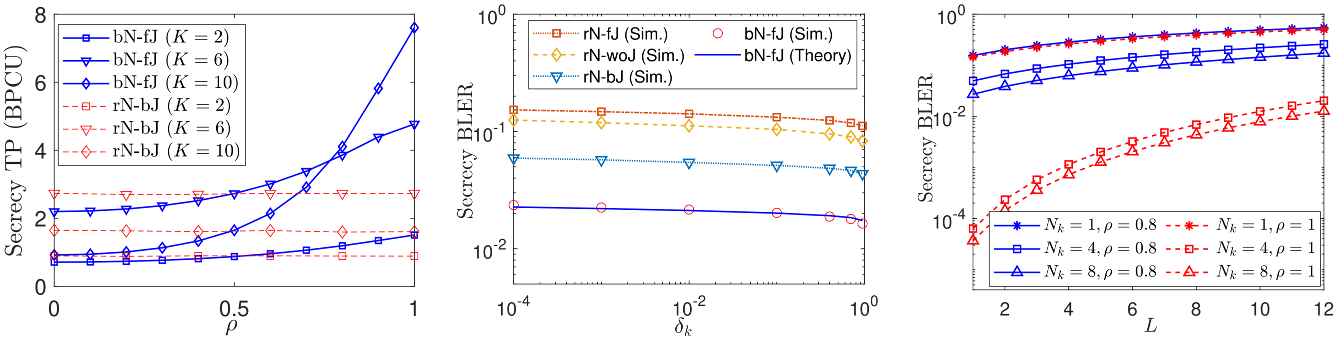


(a) Secrecy throughput of different schemes versus average SNR ψ.

(b) Secrecy throughput of the proposed bN-fJ scheme versus c_T with different imperfect CSIs and $\psi = 25$ dB.

(c) Secrecy throughput of the proposed bN-fJ scheme versus K with $\psi = 20$ dB.

Fig. 2: Average secrecy throughput versus the transmit SNR ψ, blocklength c_T, and the number of hops K, where the terms 'TP' and 'BPCU' stand for 'throughput' and 'bits per channel use', respectively.



(a) Effect of ρ on secrecy throughput with different hops.

(b) Effect of δ on secrecy BLER with $N_k = 6$, $\psi = 28$ dB and $c_T = 1200$.

(c) Effect of L on secrecy BLER with $\psi = 20$ dB, $N_K = 4$, and $c_T = 1200$.

Fig. 3: Effects of imperfect CSI coefficient ρ, the information leakage δ_k, and the number of antennas at Eve L, on the secrecy performance of bN-fJ scheme.

As observed, the secrecy BLER increases as N_k increases since the more antennas deployed at the Eve, the better its opportunities of successfully combining the eavesdropping signals. However, at a fixed number of users, increasing IoT devices in each cluster can be a reasonable solution when Eve is equipped with large antennas for its eavesdropping. In addition, more number of IoT devices deployed in the perfect CSI scenario is more effective than that of an imperfect CSI one. For example, when 8 IoT devices are employed in each cluster at $L = 10$, the communication reliability is improved from $\varepsilon_{e2e} = 4.8 \times 10^{-1}$ to $\varepsilon_{e2e} = 1.4 \times 10^{-1}$ for imperfect CSI and from $\varepsilon_{e2e} = 4.5 \times 10^{-1}$ to $\varepsilon_{e2e} = 7.8 \times 10^{-3}$ for perfect CSI, approximately a 12.5 dB and 40.5 dB gain in communication reliability, respectively.

V. Conclusions

This paper proposed the bN-fJ scheme for securing short-packet multi-hop communications in IoT networks, with a focus on enhancing average secrecy throughput and communication reliability. Closed-form expressions for the secrecy throughput of the bN-fJ scheme were derived, considering imperfect CSI and the presence of a multi-antenna eavesdropper. Asymptotic analyses for extreme values of average SNR and infinite blocklength were conducted, offering valuable insights into the system configuration. Numerical results demonstrated that the proposed bN-fJ scheme surpassed benchmark schemes in terms of secrecy throughput and communication reliability. Moreover, the optimal number of blocklengths and hops maximizing the system secrecy throughput were identified under various CSI conditions. Our future work will explore cognitive radio environments, incorporating reconfigurable intelligent surfaces in IoT-based factory automation.

Appendix A
Proof of the Theorem 1

The e2e secrecy throughput over K hops transmission is expressed as [15]

$$\tau_{e2e} = r_k \prod_{k=1}^{K} \tau_k. \tag{16}$$

Our target is to obtain τ_k which can be calculated from (7) as

$$\tau_k = \int_0^{+\infty} \int_y^{+\infty} (1 - \epsilon_k(x, y)) f_{\gamma_k}(x) f_{\gamma_{\mathrm{E},k}}(y) dx dy, \tag{17}$$

where $f_X(.)$ denotes the probability density function (PDF) of X. Incorporating the Gaussian Q-function into ϵ_k complicates the procedures of deriving an exact closed-form expression for the secrecy throughput. Thus, we approximate the secrecy

BLER in (6) by using a linear approximation of the Q-function to overcome the integral in (17) as [3]

$$\epsilon(x,y) = \begin{cases} 0, & x \geq \xi_k, \\ 1/2 - s_i\sqrt{c_D}(x-\theta_k), & \vartheta_k \leq x \leq \xi_k, \\ 1, & x < \vartheta_k, \end{cases} \quad (18)$$

where $\theta_k = 2^{\sqrt{S_E(y)/c_D}Q^{-1}(\delta_k)+r_k}(1+y)-1$, $r_k = m/c_D$, $s_k = (2\pi\theta_k(\theta_k+2))^{-1/2}$, $\vartheta_k = \theta_k - 1/(2s_k\sqrt{c_D})$, and $\xi_k = \theta_k + 1/(2s_k\sqrt{c_D})$. Subsequently, substituting (18) into (17) and using the Riemann integral approximation, the secrecy throughput can be approximated as

$$\tau_k = \int_0^{+\infty} F_{\gamma_{\mathsf{E},k}}(y) f_{\gamma_k}(\omega_k(1+y)-1)\omega_k dy, \quad (19)$$

where $\omega_k = 2^{Q^{-1}(\delta_k)/\sqrt{c_D}+r_k}$ and $F_{\gamma_{\mathsf{E},k}}(.)$ denotes the cumulative distribution function (CDF) of $\gamma_{\mathsf{E},k}$. To calculate τ_k, we need to obtain the CDF of $\gamma_{\mathsf{E},k}$. It can be derived from (4) as $F_{\gamma_{\mathsf{E},k}}(y) = \Pr[\gamma_{\mathsf{E},k} < y]$, which is further expressed as

$$F_{\gamma_{\mathsf{E},k}}(y) = \int_0^{\infty} F_{\sum\limits_{l=1}^{L}|f_{k-1,l}|^2}\Big(\rho y x + \frac{y}{\psi_{\mathsf{E},k-1}}\Big) f_{|g_{k,l}|^2}(x)dx, \quad (20)$$

where $\rho = \psi_{\mathsf{E},k}/\psi_{\mathsf{E},k-1}$. By injecting the CDF of $\sum_{l=1}^{L}|f_{k,l}|^2$ and the PDF of $f_{|g_{k+1,l}|^2}$ into (20), then applying binomial expansion, it follows that

$$F_{\gamma_{\mathsf{E},k}}(x) = 1 - \sum_{l=0}^{L}\sum_{q=0}^{l}\binom{l}{q}\frac{\rho^q\psi_{E,k}^{q-l}\Gamma(1+q)}{l!\lambda_{E,J_k}\lambda_{E,k}^{l}} \times y^l \exp\Big(-\frac{y}{\lambda_{E,k}\psi_{E,k}}\Big)\Big(\frac{1}{\lambda_{E,J_k}} + \frac{y\rho}{\lambda_{E,k}}\Big)^{-q-1}, \quad (21)$$

where $\lambda_{E,k}$ and λ_{E,J_k} are the parameters from Eve to the IoT and the jammer, respectively. The best node selection strategy is employed at hop k; thus, the PDF of γ_{k,n^*} is given by [11]

$$f_{\gamma_{k,n^*}} = \sum_{n=0}^{N_k-1}\binom{N_k-1}{n}\frac{(-1)^n N_k}{(n+1)\psi_k\Omega_k}\exp\Big(-\frac{x}{\psi_k\Omega_k}\Big). \quad (22)$$

Next, by substituting (21) and (22) into (19), and after some manipulations, we obtain as

$$\tau_k = r_k\sum_{n=0}^{N_k-1}\binom{N_k-1}{n}\frac{(-1)^n N_k}{(n+1)}\exp\Big(\frac{1-\omega_k}{\psi_k\Omega_k}\Big)\Big[1 - \sum_{l=0}^{L}\binom{l}{q} \times \frac{\beta_k\Gamma(1+q)\omega_k}{l!\psi_k\Omega_k(\lambda_{E,k}\psi_{E,k})^{l-q}}\int_0^{\infty}\frac{y^l\exp(-\Upsilon_k y)}{(\beta_k+y)^{q+1}}dy\Big]. \quad (23)$$

Let I represent the integral in (23), introducing a change of variable $t = y + \beta_k$, we arrive at $I = \exp(\beta_k\Upsilon_k)\int_{\beta_k}^{\infty}\frac{(t-\beta_k)^l\exp(-\Upsilon_k t)dt}{t^{q+1}}$. Then, applying the binomial expansion, I can be written as

$$I = \exp(\beta_k\Upsilon_k)\sum_{i=0}^{l}\binom{l}{i}(-\beta_k)^{l-i}\int_{\beta_k}^{\infty}t^{i-q-1}\exp(-\Upsilon_k t)dt. \quad (24)$$

The integral in (24), denoted by $\mathcal{U}$, is solved for two separated cases, i.e., $i > q$ and $i \leq q$, with the help of [16, Eq. (3.381.3)] and [16, Eq. (3.353.1)], respectively, which results in (11). By plugging (24) with the result in (11) into (23), we obtain τ_k, presenting in $\mathcal{T}_{1,k}$ and $\mathcal{T}_{2,k}$ as shown in (9) and (10), respectively, which then injected into (16), the e2e secrecy throughput is obtained as (8).

Appendix B
Proof of the Theorem 2

At high SNR regimes, i.e., as $\psi \in \{\psi_k, \psi_E\} \to \infty$, we apply the following approximations for (9) and (10) as follows:

$$\exp(1/x) \approx 1 \,\text{as}\, x \to \infty, \sum_{n=0}^{N_k-1}\binom{N_k-1}{n}\frac{(-1)^n N_k}{n+1} = 1. \quad (25)$$

The asymptotic secrecy throughput can be obtained as

$$\tau_{\mathtt{asym}}^{\mathtt{SNR}} \overset{\psi\to\infty}{\approx} r_k\prod_{k=1}^{K}\Big[1 - \widehat{\sum}\frac{r_k N_k\Gamma(1+q)\omega_k\beta_k^{l-i+1}}{\psi_k\Omega_k(\lambda_{E,k}\psi_{E,k})^{l-q}}\mathcal{U}\Big]. \quad (26)$$

By applying the following approximation for (26): $\prod_{k=1}^{K}(1-x_k) \approx 1 - \sum_{k=1}^{K}x_k$ for small x_k, the $\tau_{\mathtt{asym}}^{\mathtt{SNR}}$ is obtained as (14).

References

[1] P. Popovski, J. J. Nielsen, C. Stefanovic, E. De Carvalho, E. Strom, K. F. Trillingsgaard, A.-S. Bana, D. M. Kim, R. Kotaba, J. Park *et al.*, "Wireless access for ultra-reliable low-latency communication: Principles and building blocks," *IEEE Network*, vol. 32, no. 2, pp. 16–23, 2018.

[2] C. Feng, H.-M. Wang, and H. V. Poor, "Reliable and secure short-packet communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1913–1926, 2021.

[3] C. D. Ho, T.-V. Nguyen, T. Huynh-The, T.-T. Nguyen, D. B. da Costa, and B. An, "Short-packet communications in wireless-powered cognitive IoT networks: Performance analysis and deep learning evaluation," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2894–2899, Mar. 2021.

[4] N. Arı, N. Thomos, and L. Musavian, "Performance analysis of short packet communications with multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6778–6789, 2022.

[5] X. Lai, T. Wu, Q. Zhang, and J. Qin, "Average secure BLER analysis of NOMA downlink short-packet communication systems in flat Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 2948–2960, May 2021.

[6] C. Feng and H.-M. Wang, "Secure short-packet communications at the physical layer for 5G and beyond," *IEEE Commun. Standards Mag.*, vol. 5, no. 3, pp. 96–102, 2021.

[7] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Natl. Acad. Sci.*, vol. 114, no. 1, pp. 19–26, 2017.

[8] H.-M. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure short-packet communications for mission-critical IoT applications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2565–2578, May 2019.

[9] 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.

[10] D. Xu and H. Zhu, "Proactive eavesdropping via jamming over short packet suspicious communications with finite blocklength," *IEEE Trans. Commun.*, vol. 70, no. 11, pp. 7505–7519, Nov. 2022.

[11] T.-V. Nguyen, T.-H. Vu, T. Huynh-The, and D. B. Da Costa, "Secrecy performance of short-packet communications in multihop IoT networks with imperfect CSI," *IEEE Wireless Commun. Lett,*, 2024.

[12] Z. Abdullah, G. Chen, M. A. Abdullah, and J. A. Chambers, "Enhanced secrecy performance of multihop IoT networks with cooperative hybrid-duplex jamming," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 161–172, 2020.

[13] W. Yang, R. F. Schaefer, and H. V. Poor, "Finite-blocklength bounds for wiretap channels," in *2016 IEEE Int. Symp. Inf. Theory - Proc.* IEEE, pp. 10–15.

[14] A. A. Alkheir and M. Ibnkahla, "An accurate approximation of the exponential integral function using a sum of exponentials," *IEEE Commun. lett.*, vol. 17, no. 7, pp. 1364–1367, Jul. 2013.

[15] T.-V. Nguyen, V.-D. Nguyen, D. B. da Costa, T. Huynh-The, R. Q. Hu, and B. An, "Short-packet communications in multihop networks with WET: Performance analysis and deep learning-aided optimization," *IEEE Trans. Wireless Commun.*, vol. 22, no. 1, pp. 439–456, Jan. 2023.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic Press, 2007.