

Physical Layer Security of Spatially Modulated Sparse-Code Multiple Access in Aeronautical *Ad-hoc* Networking

Yusha Liu, *Student Member, IEEE*, Yuli Yang, *Senior Member, IEEE*, Lie-Liang Yang, *Fellow, IEEE* and Lajos Hanzo, *Fellow, IEEE*

Abstract—For improving the throughput while simultaneously enhancing the security in aeronautical *ad-hoc* networking (AANET), a channel quality indicator (CQI)-mapped spatially modulated sparse code multiple access (SM-SCMA) scheme is proposed in this paper. On one hand, we exploit the joint benefits of spatial modulation and SCMA for boosting the data rate. On the other hand, a physical-layer secret key is generated by varying the SM-SCMA mapping patterns based on the instantaneous CQI in the desired link. This guarantees the security of AANETs, since this secret key is not exchanged between the source aeroplane and its destination. Due to the line-of-sight (LoS) propagation in the AANET, other aeroplanes or eavesdroppers may detect the signals delivered in the desired link. However, they are unable to translate the detected signals into the original confidential information, even if multiple copies of the signals are received over multiple hops of the AANET, because they have no knowledge of the CQI-based SM-SCMA mapping pattern. The performance of the CQI-mapped SM-SCMA is evaluated in terms of both its bit error rate and its ergodic secrecy rate, which substantiates that the proposed scheme secures the confidential information exchange in the multi-hop AANET.

Index Terms—Aeronautical *ad-hoc* networking (AANET), physical layer security (PLS), sparse code multiple access (SCMA), spatial modulation (SM).

I. INTRODUCTION

As an attractive large-scale multi-hop wireless architecture, the concept of aeronautical *ad-hoc* networking (AANET) has been developed relying on multi-hop aircraft-to-aircraft (A2A) communications [1], [2]. This concept extends the coverage of wireless networks purely relying on air-to-ground communications, as well as allowing aeroplanes to assist each other in forwarding information when en-route. In practice, we can enhance the network's performance by exploiting that in many practical scenarios passenger aircrafts follow semi-deterministic routes [3]. This is particularly so for example in Trans-Atlantic scenarios, where the planes follow each other along the same flight-path at a similar velocity. This makes the

Doppler shift in A2A communications much smaller than that in air-to-ground communications, since the relative velocity between a pair of aeroplanes, specifically in the same cruising direction, is much lower than that between an aeroplane and a ground station. Thanks to the longer coherence time associated with the smaller Doppler spread in A2A communications, the time-division duplex (TDD) mode can be exploited in the AANET to boost the resource utilisation efficiency [4].

Two major challenges in the AANET are: (i) to provide hundreds of passengers in the cabin with fast Internet access, which requires extremely high throughput in the A2A links; and (ii) to guarantee the security of control networks and Internet connectivity in the wireless communications at a high risk of data breaches, concerning the leakage of information delivered in an A2A link to the other aeroplanes or eavesdroppers due to the broadcast nature of strong line-of-sight (LoS) propagation [5] associated with multiple plane-to-plane transmissions.

Traditional network security relies on upper-layer encryption for the confidentiality and authenticity of communications. However, the higher-layer secret key exchange requires extra communication resources, thereby reducing the throughput. Moreover, the cryptographic technologies implemented at the upper layers are not suitable for the high-dynamic infrastructure of the AANET, where communications over the A2A links can be guaranteed by physical layer security (PLS). Compared to traditional network security, PLS has a number of merits. Firstly, the inherent random characteristics of wireless channels is exploited to guarantee information confidentiality [6]–[8]. Since the third parties have no knowledge of the legitimate channel state information (CSI), they cannot decode the confidential information. Secondly, the third parties' channels are degraded in the PLS mechanism, by beamforming [9]–[11], artificial noise [12], jamming [13]–[15] or cooperative relaying [16], [17]. Furthermore, PLS techniques avoid wasteful signal processing routinely required for upper-layer secret key exchange, therefore boosting the resource utilisation efficiency. Finally, PLS is also compatible with upper-layer encryption required for ultimate security.

Against this backdrop, the PLS mechanism is exploited for enhancing the security of AANETs while simultaneously improving both the resource utilisation efficiency and the throughput [18], [19]. In particular, the spatial-domain resources formed by multi-antenna configurations are exploited for conceiving spatial modulation (SM) assisted PLS [20].

Y. Liu, L. Yang, and L. Hanzo are with the school of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: yl6g15@ecs.soton.ac.uk, lly@ecs.soton.ac.uk, lh@ecs.soton.ac.uk).

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

The financial support of the Engineering and Physical Sciences Research Council project EP/P034284/1 is gratefully acknowledged.

L. Hanzo would like to gratefully acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/Noo4558/1, EP/P034284/1, COALESCE, of the Royal Society's Global Challenges Research Fund Grant as well as of the European Research Council's Advanced Fellow Grant QuantCom.

TABLE I
OVERVIEW OF EXISTING LITERATURE.

Contributions	This work	[21], [22]	[23]	[24]	[25]	[29]	[30]-[32]	[39]-[42]
Aeronautical <i>Ad-hoc</i> Networking (AANET)	✓							
Multi-hop networks	✓							
Physical Layer Security (PLS)	✓	✓	✓	✓	✓			✓
Non-Orthogonal Multiple Access (NOMA)	✓					✓	✓	✓
Spatial Modulation (SM)	✓	✓	✓	✓	✓	✓	✓	
CQI-based Bit-to-Symbol Mapping	✓				✓			
Multi-Carrier (MC) Transmissions	✓						✓	

In this context, Wu *et al.* [21], [22] proposed a precoding-aided SM scheme for secrecy communications in by jointly maximizing the signal power at the desired receiver and minimizing the power received at the eavesdropper. Wang *et al.* [23] adopted jamming techniques for improving the secrecy rate of secure SM communications. A design alternative for increasing the secrecy rate of SM-assisted PLS was proposed in [24] by relying on transmit antenna (TA) selection, which further reduces the number of radio frequency (RF) chains required by the SM configurations.

Although these solutions may guarantee secure communications, they are not so suitable for enhancing the PLS of AANETs since they rely on the knowledge of the wiretapping CSI for degrading the wiretapper link. In the AANET, to obtain the CSI of third parties would require excessive extra communication resources. Moreover, the strong LoS propagation of the A2A links facilitates the third parties' wiretapping and it would require quite a high power to jam the eavesdroppers. A physical-layer secret key generation method was proposed in [25] for enhancing the PLS by degrading the eavesdroppers' detection quality without requiring the wiretapper's CSI. Motivated by this, we develop a mapping-aided SM-assisted PLS solution for AANETs. The SM mapping patterns are varied according to the instantaneous channel quality indicator (CQI) of the link spanning from the transmitter to the desired receiver, which are used as the secret key. Given the channel reciprocity of the TDD mode considered, the CQI is not transmitted in the feedback channel. Since the third parties cannot obtain the CQI of the desired link, they have no basis for decoding the confidential information, even if they can detect the signals transmitted over this link. Our solution is ideally suited for AANETs.

In parallel with the advances of PLS in the AANET, increasing the data rate of A2A links is our second main objective. One approach is to adopt multiple transmit antennas, as investigated in [26], [27]. An alternative solution is employing non-orthogonal multiple access (NOMA) techniques [28], where multiple data streams are conveyed by a single orthogonal resource. The investigations of various NOMA schemes in combination with SM have demonstrated promising complexity reductions compared to the conventional multi-antenna NOMA systems, mainly owing to the reduced number of RF chains. In [29], Wang *et al.* investigated a general NOMA scheme relying on SM for downlink transmission. As

a further advance, Liu *et al.* [30]–[32] adopted a code-domain NOMA technique, i.e., sparse-code multiple access (SCMA) [33], and amalgamated with SM for conceiving SM-SCMA for supporting the heavily loaded Internet-of-Things. Low complexity detection algorithms proposed in [34], [35] further facilitate the potential application of SM-SCMA schemes in AANETs. In [36], a cooperative SM-NOMA scheme was introduced into vehicle-to-vehicle networks and its performance was investigated. The benefits of SM-NOMA may also be combined with those of *ad-hoc* networks, where low latency is required, despite the impediments of multi-hop transmissions [37], [38]. To improve the security performance, several PLS techniques have been investigated in NOMA systems [39]–[42]. However, there is a paucity in literature on the PLS of SM-NOMA systems, especially in the AANET context.

Against this background, we propose a CQI-mapped SM-SCMA scheme for enhancing the PLS of multi-hop AANETs. The novelty of our work is boldly and explicitly compared to the state-of-the-art in Table I at a glance. The main contributions of this paper are summarized as follows.

- We propose a CQI-mapped SM-SCMA scheme for achieving high throughput, while enhancing the PLS in multihop AANETs, where the SM-SCMA mapping pattern is varied according to the instantaneous CQI of the desired link, which is then used as a physical-layer secret key. Since the SM and SCMA are directly selected according to the instantaneous CQI, no extra computations are required for obtaining the secret key. Additionally, the proposed scheme achieves a high data rate by transmitting multiple data streams through a single resource and by conveying extra information through the TA index.
- The specific channel characteristics of AANETs are taken into account in our design. Explicitly, the strong LoS propagation improves Eve's detection performance, who also benefits from intercepting multiple copies of the signal during multi-hop relaying. As a compelling benefit of the proposed scheme, eavesdroppers cannot extract the confidential information, since they do not know the CQI of the desired link. This guarantees secure communications in AANETs, despite its strong LoS propagation and its multi-hop nature.
- The performance of our CQI-mapped SM-SCMA is evaluated in terms of its bit error rate (BER), ergodic data

rate, ergodic secrecy rate and detection complexity within the multi-hop AANETs. Our numerical results substantiate the benefits of the proposed scheme in achieving a high throughput, while simultaneously enhancing the PLS of the AANETs.

The remainder of this paper is organized as follows. Firstly, Section II proposes the CQI-mapped SM-SCMA for enhancing both the throughput and the PLS of AANETs. A turbo-coded system is presented. Subsequently, Section III presents the signal detection and decoding at both the desired receiver and the third parties. To evaluate performance of our proposed scheme in multi-hop AANETs, its secrecy rate is formulated in Section IV, followed by our simulation results characterizing both the BER and ergodic secrecy rate in Section V. Finally, this paper is concluded in Section VI.

Notations: Matrices and vectors are denoted by boldface uppercase and lowercase letters, respectively. In particular, $\mathbf{0}_{M \times 1}$ denotes the $M \times 1$ zero vector and \mathbf{I}_M denotes the $M \times M$ identity matrix. The transpose, the conjugate transpose and the modulus operators are denoted by $(\cdot)^T$, $(\cdot)^\dagger$ and $\|\cdot\|$, respectively. Moreover, $\mathcal{E}\{\cdot\}$ represents the expectation (mean) operator, and the conditional probability density function (PDF) of a random variable x given the event of $y = A$ is denoted by $p(x|y = A)$.

II. SYSTEM MODEL

A. Channel Modelling in AANET

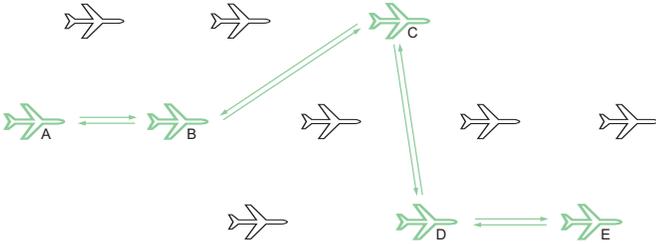


Fig. 1. A multi-hop channel in AANET.

Let us consider an AANET supporting a group of aeroplanes, as shown in Fig. 1, where a reciprocal link can be set up between any two of them and the routing from a source aeroplane to its destination hinges on the trade-off between link quality and latency. The relative velocity between the transmitter and the receiver in a reciprocal link is stable and quite low in comparison to the absolute velocity of aircraft, which results in a low Doppler shift. To boost the resource utilisation efficiency, the A2A communications adopt the TDD mode, which facilitates for multiple aeroplanes to access a shared spectral band and no wasteful guard bands are needed. Moreover, the TDD mode allows the aeroplanes to know each other's CSI without feedback channel.

The channel statistics of the AANET are composed of the signal attenuation with phase variation, the Doppler shift and the multipath effects during wave propagation. Explicitly, the channels in A2A communications are Rician-distributed, consisting of the LoS and the scattered components. The ratio

of the LoS path power to the scattered power is defined as the Rician factor $\kappa = \sigma_{\text{LoS}}^2 / \sigma_S^2$, where σ_{LoS}^2 and σ_S^2 represent the LoS path power and the scattered power generated by Clarke's model, respectively. Specifically, the power normalization requires $\sigma_{\text{LoS}}^2 + \sigma_S^2 = 1$, which gives

$$\sigma_{\text{LoS}}^2 = \sqrt{\frac{\kappa}{\kappa + 1}} \quad \text{and} \quad \sigma_S^2 = \sqrt{\frac{1}{\kappa + 1}}. \quad (1)$$

The channel characteristics in different phases of the aircraft flight, i.e., parking, taxiing, takeoff, en-route, holding, and landing, are specified in [1] and [5]. In practice, A2A communications are typically relied upon in the en-route phase, with the channel characteristics in terms of aircraft velocity v , typical Rician factor κ , maximum Doppler frequency f_d and maximum normalized Doppler frequency \bar{f}_d listed in Table II.

As shown in Table II, we adopt the Type-1 L-band Digital Aeronautical Communications System (L-DACS1) framework, which offers data services under the LTE standards [43]. The various aircraft velocities, $v \in [17, 620]$ m/s, result in Doppler shift of $f_d \in [0.056, 2.07]$ kHz, calculated by $f_d = v f_c / c$, where $c = 3 \times 10^8$ m/s is the speed of light and $f_c = 1$ GHz is the carrier frequency employed in L-DACS1. This results in the maximum normalized Doppler shifts of $\bar{f}_d \in [0.896 \times 10^{-4}, 33.1 \times 10^{-4}]$, calculated by $\bar{f}_d = f_d / f_s$, where $f_s = 625$ kHz is the Baud rate of the L-DACS1 [43].

Given the aircraft velocity $v \ll c$, the Doppler shift in an A2A link can be calculated using $\Delta f = \Delta v \cdot f_c / c$, where Δv is the relative velocity between the transmitter and the receiver. In practice, Δv within an A2A link is controllable. Assuming that Δv follows a normal distribution with the mean of 30 m/s and a certain variance less than 30 m/s, the mean Doppler shift is 0.1 kHz in this A2A link. If the mean of Δv is predictable, the Doppler shift contributed by it can be compensated through a frequency pre-shift at the transmitter. As such, the Doppler spread results from the variational components of Δv and the scattered multipath components, which means that the minimum coherence time is 10 ms. Therefore, when the TDD mode is employed, the minimum duration of a single time slot is 5 ms.

For the multi-hop AANET portrayed in Fig. 1, we assume that the information exchange between Aeroplanes A and E is routed via B, C, and D, hence forming the trajectory of A-B-C-D-E, given the link quality and latency table of the relevant moment. However, when Aeroplane A transmits its signal to Aeroplane B, the other nearby aeroplanes in this AANET can detect and decode the signals forwarded in this path, which will result in security threats.

B. CQI-mapped SM-SCMA

Now we consider A2A communications over a single hop in the AANET. The system model of the proposed CQI-mapped turbo-encoded SM-SCMA over the t -th ($t = 1, 2, \dots, T$) hop in a routed path within the AANET is illustrated in Fig. 2, where an eavesdropper attempts to extract the confidential information delivered via this link. The transmitter has M TAs and employs R subcarriers. There are N receive antennas (RAs) and N_E RAs at the eavesdropper. The r^{th} subcarrier

TABLE II
CHANNEL CHARACTERISTICS OF THE A2A COMMUNICATIONS IN THE EN-ROUTE PHASE.

Characteristics		κ (dB)	v (m/s)	f_d (kHz)	$\bar{f}_d (\times 10^{-4})$
L-DACS1 [43]	Range	2 - 20	17 - 620	0.056 - 2.07	0.896 - 33.1
	Example	15	30	0.1	1.6

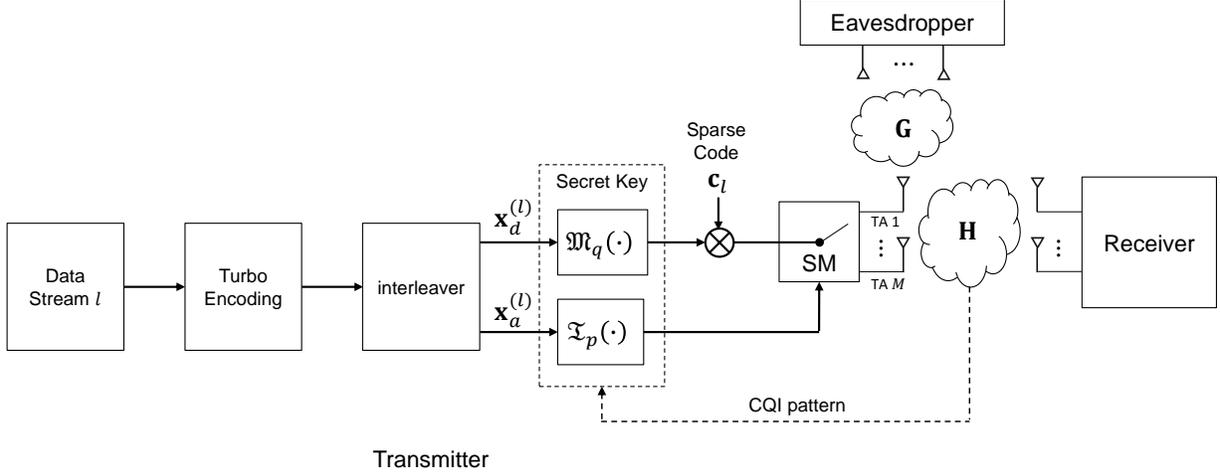


Fig. 2. The CQI-mapped SM-SCMA with turbo encoding for the l^{th} data stream delivered over a hop in the AANET.

channels spanning from the transmitter to the receiver and the eavesdropper are denoted by a $N \times M$ matrix $\mathbf{H}_r = [h_{nm}^{(r)}]_{N \times M} = [\mathbf{h}_1^{(r)}, \mathbf{h}_2^{(r)}, \dots, \mathbf{h}_M^{(r)}]$ and a $N_E \times M$ matrix $\mathbf{G}_r = [g_{nm}^{(r)}]_{N_E \times M} = [\mathbf{g}_1^{(r)}, \mathbf{g}_2^{(r)}, \dots, \mathbf{g}_M^{(r)}]$, respectively, where the $N \times 1$ vector $\mathbf{h}_m^{(r)} = [h_{1m}^{(r)}, h_{2m}^{(r)}, \dots, h_{Nm}^{(r)}]^T$ contains the channel coefficients from the m^{th} TA to all RAs, and the $N_E \times 1$ vector $\mathbf{g}_m^{(r)} = [g_{1m}^{(r)}, g_{2m}^{(r)}, \dots, g_{N_E m}^{(r)}]^T$ contains the channel coefficients from the m^{th} TA to all RAs of the eavesdropper, in the r^{th} subcarrier over this hop, $m = 1, 2, \dots, M$, $n = 1, 2, \dots, N_E$, $r = 1, 2, \dots, R$.

Within the AANET, the Rician channel vectors $\mathbf{h}_m^{(r)}$ and $\mathbf{g}_m^{(r)}$ are expressed as

$$\mathbf{h}_m^{(r)} = \sqrt{\frac{\kappa}{\kappa+1}} \mathbf{e}_{N \times 1} + \sqrt{\frac{1}{\kappa+1}} \tilde{\mathbf{h}}_m^{(r)} \quad (2)$$

and

$$\mathbf{g}_m^{(r)} = \sqrt{\frac{\kappa}{\kappa+1}} \mathbf{e}_{N_E \times 1} + \sqrt{\frac{1}{\kappa+1}} \tilde{\mathbf{g}}_m^{(r)}, \quad (3)$$

respectively, where the LoS paths $\mathbf{e}_{N \times 1}$ and $\mathbf{e}_{N_E \times 1}$ are all-one vectors. The $N \times 1$ vector $\tilde{\mathbf{h}}_m^{(r)} \sim \mathcal{CN}(\mathbf{0}_{N \times 1}, \mathbf{I}_N)$ and the $N_E \times 1$ vector $\tilde{\mathbf{g}}_m^{(r)} \sim \mathcal{CN}(\mathbf{0}_{N_E \times 1}, \mathbf{I}_{N_E})$ contain i.i.d. complex Gaussian random variables with zero-mean and unit variance in the scattered components.

In this hop, the CQI from the m^{th} TA to all RAs in the r^{th} subcarrier is denoted by $\gamma_m^{(r)} = (\mathbf{h}_m^{(r)})^\dagger (\mathbf{h}_m^{(r)})$, where $m \in \{1, 2, \dots, M\}$, $r = 1, 2, \dots, R$; thus, the CQI pattern in this subcarrier is given by the permutation containing all $\gamma_m^{(r)}$, i.e., $m = 1, 2, \dots, M$, in descending or ascending order. For example, in the case of $M = 2$, there are two CQI patterns for each subcarrier, i.e., Pattern 1 is $\gamma_1^{(r)} > \gamma_2^{(r)}$ and Pattern 2 is $\gamma_2^{(r)} > \gamma_1^{(r)}$. In the case of $M = 4$, there

are 24 permutations of the 4 CQIs in each subcarrier, i.e., $\gamma_1^{(r)} > \gamma_2^{(r)} > \gamma_3^{(r)} > \gamma_4^{(r)}$, $\gamma_4^{(r)} > \gamma_3^{(r)} > \gamma_2^{(r)} > \gamma_1^{(r)}$, and so on. From an ergodic view point, the total number of CQI patterns in each subcarrier is $P = M!$ and each pattern occurs at the same probability.

To improve the throughput, SCMA is employed to deliver L data streams simultaneously over R orthogonal subcarriers ($L > R$), and SM is utilised to activate a specific TA by a fraction of the information bits.

For the sake of improving the PLS, the transmitter exploits our CQI-mapped SM-SCMA to form its SM and SCMA mapping patterns according to the instantaneous CQI pattern of the desired link \mathbf{H}_r , which is equivalent to generating a secret physical-layer key via the CQI pattern in this hop [25]. In contrast to precoding or jamming, the bit-to-symbol mapping patterns in SM-SCMA are determined by the CQI pattern in \mathbf{H}_r for each instant or channel use, which does not require any extra transmit power for precoding or artificial noise. Thanks to the channel reciprocity of the TDD mode, no feedback channel is needed to deliver the CQI and, therefore, only the transmitter and the desired receiver of this hop know the CQI pattern as well as the SM and SCMA mapping patterns of each channel use. All the other aeroplanes within the AANET and all the outside eavesdroppers have no information on this secret key; thus they will fail to detect the information conveyed in this hop, since they do not have the correct bit-to-symbol mapping patterns to decode their received SM-SCMA signals.

The delivery of the l^{th} data stream, $l = 1, 2, \dots, L$, at the transmitter is shown in Fig. 2, where the A -length data stream \mathbf{u}_l is firstly turbo-encoded into a E -length coded bit sequence \mathbf{b}_l , giving a coding rate of E/A .

After interleaving the coded bit sequence, the interleaved bit sequence $\mathbf{b}_l = \pi(\bar{\mathbf{b}}_l)$ is divided into F groups $\mathbf{x}_l^{(1)}, \mathbf{x}_l^{(2)}, \dots, \mathbf{x}_l^{(F)}$, and then mapped onto F SM-SCMA symbols. Since these symbols are formed by the same SM-SCMA mapping pattern, in the following we omit the superscript (f) , $f = 1, 2, \dots, F$, unless it is required. A bit group \mathbf{x}_l is split into two portions for SM and SCMA, i.e., $\mathbf{x}_l = [\mathbf{x}_a^{(l)}, \mathbf{x}_d^{(l)}]$, where $\mathbf{x}_a^{(l)}$ and $\mathbf{x}_d^{(l)}$ are the $\log_2 M$ bits mapped onto the TA indices and the $\log_2 K$ radiated bits mapped onto classic amplitude/phase-modulation (APM) symbols, respectively. The number of TA-selection patterns is equal to the number of CQI patterns in a subcarrier, $P = M!$, and the number of APM mapping patterns is $Q = K!$, where K is the APM order. More specifically, for a $R \times L$ SCMA supporting L data streams by R orthogonal subcarriers, the l^{th} data stream will be mapped to one of its Q SCMA codebook patterns, according to the CQI of \mathbf{H} and will be transmitted by the $d_l \ll R$ orthogonal subcarriers that are pre-assigned to the l^{th} data stream. An example of the subcarrier assignment matrix \mathbf{C} of the 4×6 SCMA supporting $L = 6$ data streams using $R = 4$ subcarriers can be expressed as

$$\mathbf{C} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \quad (4)$$

In this example, there are 2 orthogonal subcarriers assigned to a single data stream, i.e., $d_l = 2$, and the number of data streams sharing the same subcarrier is $d_r = 3$.

During an arbitrary transmission, if the p^{th} CQI pattern occurs in the hop-channel \mathbf{H} , the transmitter will exploit the p^{th} TA-selection pattern, denoted by $\mathfrak{T}_p^{(l)}(\cdot)$, $p \in \{1, 2, \dots, P\}$, and the q^{th} SCMA mapping pattern for the l^{th} data stream conveyed by the r^{th} subcarrier, denoted by $\mathfrak{M}_q^{(l,r)}(\cdot)$, $q \in \{1, 2, \dots, Q\}$. An instance of the 4×6 SM-SCMA mapping patterns varying with the CQI pattern for the first data stream is illustrated in Fig. 3, where the transmitter has $M = 2$ TAs with $K = 4$ for SCMA and there are $P = 2$ CQI patterns for each subcarrier. With the SCMA characterized by (4), the first data stream is delivered through Subcarriers 1 and 2. If Pattern 1, $\gamma_1^{(r)} > \gamma_2^{(r)}$, occurs in Subcarrier r ($r = 1, 2$), the SM-SCMA mapping patterns are given by Fig. 3 (a), where bit 0 is mapped by TA 1 and bit 1 is mapped by TA 2, denoted by $\text{TA } 1 \leftrightarrow 0$ and $\text{TA } 2 \leftrightarrow 1$. If Pattern 2, $\gamma_1^{(r)} < \gamma_2^{(r)}$, occurs in Subcarrier r , the SM-SCMA mapping patterns are given by Fig. 3 (b).

Hence, the $N \times 1$ baseband signals at the r^{th} subcarrier received by the desired receiver is obtained by

$$\mathbf{y}_r = \sum_{l \in \{l_1^{(r)}, l_2^{(r)}, l_3^{(r)}\}} \mathbf{h}_{\mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)})}^{(r)} e^{j\theta_{\mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)})}(\mathbf{x}_a^{(l)})} \mathfrak{M}_q^{(l,r)}(\mathbf{x}_d^{(l)}) + \mathbf{z}_r, \quad (5)$$

where the set $\{l_1^{(r)}, l_2^{(r)}, l_3^{(r)}\}$ contains the indices of the 3 data streams sharing the r^{th} subcarrier, and the $N \times 1$ vector $\mathbf{z}_r \sim \mathcal{CN}(\mathbf{0}_{N \times 1}, \sigma_z^2 \mathbf{I}_N)$ contains the additive white Gaussian noise (AWGN) components. The subscript $\mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)})$ denotes the index of the TA activated by $\mathbf{x}_a^{(l)}$ according to

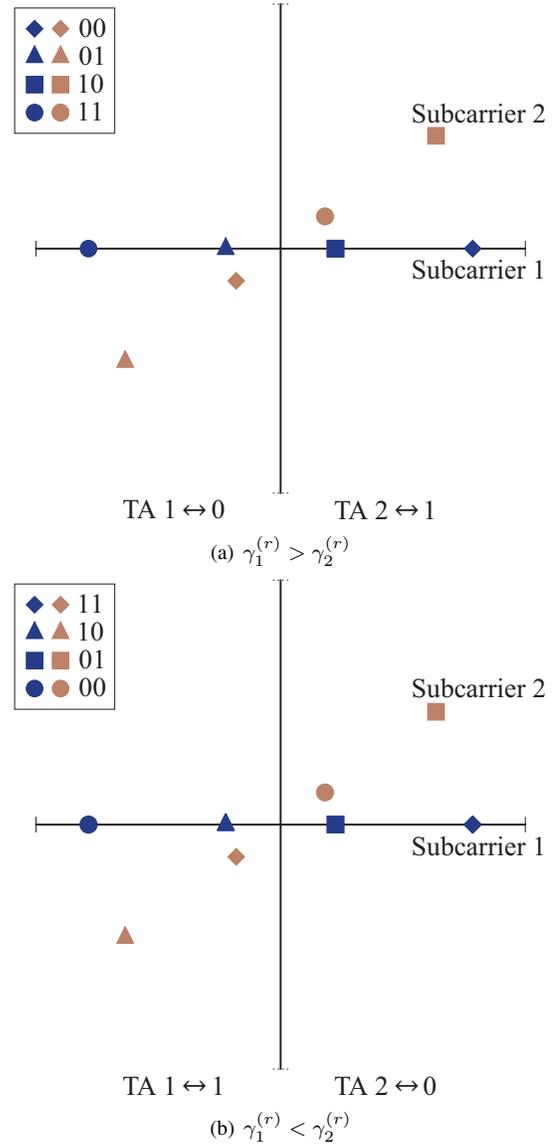


Fig. 3. An example of the 4×6 SM-SCMA mapping patterns for the first data stream at Subcarriers 1 and 2 ($r = 1, 2$), where the number of TAs, $M = 2$, and the APM order $K = 4$.

the p^{th} antenna-selection pattern. Therefore, the $N \times 1$ vector $\mathbf{h}_{\mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)})}^{(r)}$ contains the channel coefficients from the activated TA of the transmitter to the receiver at the r^{th} subcarrier. Moreover, $\mathfrak{M}_q^{(l,r)}(\mathbf{x}_d^{(l)})$ is the SCMA symbol in the l^{th} data stream transmitted over the r^{th} subcarrier, which is mapped by $\mathbf{x}_d^{(l)}$ according to the q^{th} SCMA mapping pattern, $\mathfrak{M}_q^{(l,r)}(\cdot)$. To improve the SM performance in Rician channels, we impose a phase rotation on the 4×6 SCMA symbols to distinguish the different TAs [44], i.e., $\theta_m = 2\pi(m-1)/(3MR)$, $m = 1, 2, \dots, M$. In this equation, $\theta_{\mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)})}$ is the phase rotation of the TA $\mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)})$.

Similarly, the baseband signals at the r^{th} subcarrier received

by the eavesdropper are given by

$$\mathbf{y}_E^{(r)} = \sum_{l \in \{l_1^{(r)}, l_2^{(r)}, l_3^{(r)}\}} \mathbf{g}_{\mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)})}^{(r)} e^{j\theta_{\mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)})}} \mathfrak{M}_q^{(l,r)}(\mathbf{x}_d^{(l)}) + \mathbf{z}_E^{(r)}, \quad (6)$$

where the $N_E \times 1$ vectors $\mathbf{y}_E^{(r)}$ and $\mathbf{z}_E^{(r)} \sim \mathcal{CN}(\mathbf{0}_{N \times 1}, \sigma_Z^2 \mathbf{I}_N)$ contain the eavesdropper's received signals and the AWGN components, respectively.

III. SIGNAL DETECTION

In this section, the detection of CQI-mapped SM-SCMA signals are presented for both the desired receiver and the third party to quantify the PLS of AANETs with our proposed scheme from the decoding perspective. Since the length of TDD frames is designed in terms of the channel's coherence time, as stated in Section II-A, the CSI is assumed herein to be perfectly known both at the desired receiver and at the eavesdroppers.

A. Desired Receiver

The channel's reciprocity of the TDD mode allows the desired receiver at any hop to always exploit the instantaneous CQI pattern in this hop. Hence, the SM and SCMA mapping patterns are always known to the desired receiver at any hop in the AANET.

The desired receiver's detection relies on the message passing algorithm (MPA) proposed in [31]. Explicitly, the MPA detection exploits the information propagating via the connections between the L data streams and the R subcarriers, which can be visualized by a factor graph, comprising L variable nodes (VNs) and R check nodes (CNs), as exemplified in Fig. 4, where we have $R = 4$, $L = 6$, $d_l = 2$ and $d_r = 3$. The connection between VN l and CN r is denoted by $\epsilon_{l,r}$.

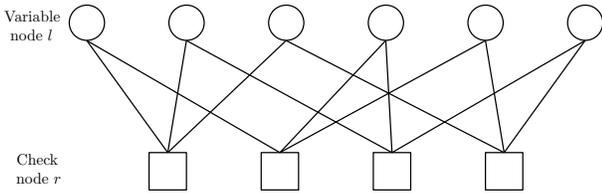


Fig. 4. An example of the factor graph of the proposed SM-SCMA scheme with the parameters $R = 4$, $L = 6$, $d_l = 2$ and $d_r = 3$.

Before detailing the MPA detection, we first define the connections to VN l and those to CN r in the factor graph into two sets, which can be respectively expressed as

$$\mathcal{V}_l = \{r : 1 \leq r \leq R, \epsilon_{l,r} \neq 0\}, l = 1, \dots, L, \quad (7)$$

$$\mathcal{C}_r = \{l : 1 \leq l \leq L, \epsilon_{l,r} \neq 0\}, r = 1, \dots, R. \quad (8)$$

Furthermore, $\delta_{r \rightarrow l}^{(w,i)} [w = \mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)}) | \mathfrak{M}_q^{(l,r)}(\mathbf{x}_d^{(l)})]$ is defined as the information conveyed from CN r to VN l during the i^{th} iteration of the MPA detection, which represents the likelihood of $w = \mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)}) | \mathfrak{M}_q^{(l,r)}(\mathbf{x}_d^{(l)})$, given all likelihoods received by CN r from all connected VNs $[r]$ excluding VN l , namely $[r] \setminus l \in \{\mathcal{C}_r \setminus l\}$ with ' \setminus ' denoting the exclusion operation. By

contrast, the likelihood forwarded from VN l to CN r in the i^{th} iteration is defined as $\eta_{l \rightarrow r}^{(w,i)}$, which represents the probability of $w = \mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)}) | \mathfrak{M}_q^{(l,r)}(\mathbf{x}_d^{(l)})$ given the probabilities received by VN l from all connected CNs $[l]$ excluding CN r , i.e., $[l] \setminus r \in \{\mathcal{V}_l \setminus r\}$. Then the MPA detection operates in the following steps:

1) *Initialisation*: Given the equiprobable transmission of all SM-SCMA symbols, $\eta_{l \rightarrow r}^{(w,0)}$ is initialised to $1/(MK)$ for any $\epsilon_{l,r} \neq 0$ and for all $w = \mathfrak{T}_p^{(l)}(\mathbf{x}_a^{(l)}) | \mathfrak{M}_q^{(l,r)}(\mathbf{x}_d^{(l)}) \in \mathfrak{S}_{p,q}^{(l,r)}(\cdot)$, where $\mathfrak{S}_{p,q}^{(l,r)}(\cdot) \triangleq \mathfrak{T}_p^{(l)}(\cdot) \otimes \mathfrak{M}_q^{(l,r)}(\cdot)$ represents the combination the p^{th} SM mapping pattern and the q^{th} SCMA mapping pattern for the l^{th} data stream, with \otimes denoting the Kronecker product.

2) *VN update*: At the i^{th} iteration, the information conveyed by CN r to VN l , i.e. $\delta_{r \rightarrow l}^{(w,i)}$ for $l \in \mathcal{C}_r$, is updated as

$$\delta_{r \rightarrow l}^{(w,i)} = \sum_{\mathbf{x}_{[r]} \in \mathfrak{S}(\mathcal{C}_r \setminus l, r)(\cdot)} \left(\prod_{\mathbf{x}^{(l')} \in \mathbf{x}_{[r]} \setminus \mathbf{x}^{(l)}} \eta_{l' \rightarrow r}^{(w,i)} \right) \prod_{n=1}^N p(y_n^{(r)} | \mathbf{x}_{[r]}), \quad (9)$$

where $\prod_{\mathbf{x}^{(l')} \in \mathbf{x}_{[r]} \setminus \mathbf{x}^{(l)}} \eta_{l' \rightarrow r}^{(w,i)}$ is the product of the probabilities propagated to CN r from all connected VNs excluding VN l , i.e., the *a priori* probability of a given $\mathbf{x}_{[r]} \setminus \mathbf{x}^{(l)}$ with $w = \mathbf{x}^{(l')}$, and $\mathfrak{S}(\mathcal{C}_r \setminus l, r)(\cdot)$ represents the SM-SCMA mapping patterns of the data streams that are connected to the r^{th} subcarrier excluding the l^{th} data stream. The conditional PDF of the r^{th} subcarrier signal received by the n^{th} antenna, $y_n^{(r)}$, given $\mathbf{x}_{[r]}$ is formulated as

$$p(y_n^{(r)} | \mathbf{x}_{[r]}) = \frac{1}{2\pi\sigma_Z^2} \exp\left(-\frac{\|y_n^{(r)} - \sum_{l' \in \mathcal{C}_r} h_{nm}^{(r)} s_r^{(l')}\|^2}{2\sigma_Z^2}\right), \quad (10)$$

where $s_r^{(l')} \in \mathfrak{M}_q^{(l',r)}(\cdot)$ is the APM signal mapped by the q^{th} SCMA mapping pattern of data stream l' at the r^{th} subcarrier.

3) *CN update*: At the $(i+1)^{\text{th}}$ iteration, $\delta_{r \rightarrow l}^{(w,i+1)}$ obtained in the i^{th} iteration is used to update $\eta_{l \rightarrow r}^{(w,i+1)}$, expressed as

$$\eta_{l \rightarrow r}^{(w,i+1)} = \epsilon_{l,r} \prod_{r' \in \mathcal{V}_l \setminus r} \delta_{r' \rightarrow l}^{(w,i)}, \quad (11)$$

where $\epsilon_{l,r}$ is the normalisation factor enabling $\sum_{w \in \mathfrak{S}_{p,q}^{(l,r)}(\cdot)} \eta_{l \rightarrow r}^{(w,i+1)} = 1$.

4) *Log-Likelihood Ratio (LLR) Conversion*: Once the predetermined number of iterations, I , is reached, the symbol probability $\eta_l^{(w,I)}$ of the l^{th} data stream according to the mapping pattern of the moment, $\forall w \in \mathfrak{S}_{p,q}^{(l,r)}(\cdot)$, is expressed as

$$\eta_l^{(w,I)} = \prod_{r \in \mathcal{V}_l} \delta_{r \rightarrow l}^{(w,I)}. \quad (12)$$

As a result, the symbol probability $\eta_l^{(w,I)}$ is converted to a *posteriori* bit LLRs given by

$$L^{post,MPA}(\hat{b}_v^{(l)}) = \ln \frac{\sum_{w \in \mathfrak{S}_{p,q}^{(l,r)}(\cdot), \hat{b}_v^{(l)}=0} \eta_l^{(w,I)}}{\sum_{w \in \mathfrak{S}_{p,q}^{(l,r)}(\cdot), \hat{b}_v^{(l)}=1} \eta_l^{(w,I)}}, \quad (13)$$

where $\hat{b}_v^{(l)}$ is the v^{th} bit of the detected SM-SCMA symbol in the l^{th} data stream, $w \in \mathfrak{S}_{p,q}^{(l,r)}(\cdot)$. Then, the *extrinsic* information of $\hat{b}_v^{(l)}$ is obtained by

$$\begin{aligned} L^{e,\text{MPA}}(\hat{b}_v^{(l)}) &= L^{\text{post,MPA}}(\hat{b}_v^{(l)}) - L^{a,\text{MPA}}(\hat{b}_v^{(l)}) \\ &= \ln \frac{\sum_{w \in \mathfrak{S}_{p,q}^{(l,r)}(\cdot), \hat{b}_v^{(l)}=0} \eta_l^{(w,I)}}{\sum_{w \in \mathfrak{S}_{p,q}^{(l,r)}(\cdot), \hat{b}_v^{(l)}=1} \eta_l^{(w,I)}} - \ln \frac{p(\hat{b}_v^{(l)}=0)}{p(\hat{b}_v^{(l)}=1)}, \end{aligned} \quad (14)$$

where

$$L^{a,\text{MPA}}(\hat{b}_v^{(l)}) = \ln \frac{p(\hat{b}_v^{(l)}=0)}{p(\hat{b}_v^{(l)}=1)} \quad (15)$$

is the *a priori* LLR of $\hat{b}_v^{(l)}$. Given the equiprobable transmission of Bit 0 and Bit 1, we have $p(\hat{b}_v^{(l)}=0) = p(\hat{b}_v^{(l)}=1)$ and $L^{a,\text{MPA}}(\hat{b}_v^{(l)}) = 0$.

After the MPA detection of all F SM-SCMA symbols, i.e., the bit groups $\mathbf{x}_l^{(1)}, \mathbf{x}_l^{(2)}, \dots, \mathbf{x}_l^{(F)}$, the extrinsic bit LLRs $L^{e,\text{MPA}}(\hat{b}_v^{(l,f)})$ of the l^{th} data stream, $\forall f = 1, 2, \dots, F$, $v = 1, 2, \dots, A/F$, are entered into the turbo decoder after the de-interleaver for performing Log-BCJR turbo decoding at the desired receiver [45]. The decoded LLRs are then forwarded to the next hop.

In practice, there are two relaying schemes available within the multi-hop AANET, given T hops in total. One is the *detect-and-forward* scheme, where the transmitter in an intermediate hop, $t \in \{1, \dots, T-1\}$, detects its received signal in the $(t-1)^{\text{th}}$ hop and then transmits its detected signal. Herein, only the destination aeroplane performs the MPA detection followed by Log-BCJR decoding to obtain the original information of the source aeroplane. Another relaying scheme is the *detect & decode-and-forward*, where every transmitter in an intermediate hop has to perform MPA detection followed by Log-BCJR decoding based on its received signal in the former hop before forwarding the information bits it has decoded.

B. Undesired Receivers or Eavesdroppers

As shown in Fig. 2, the eavesdropper (Eve) attempts to detect the information delivered in a hop of the AANET, based on her received signal $\mathbf{y}_E^{(r)}$ given in (6).

Eve may perform the same MPA detection followed by Log-BCJR turbo decoding as the desired receiver does in Subsection III-A. However, since Eve does not know the CQI of the desired link, she cannot access the SM-SCMA mapping pattern $\mathfrak{S}_{p,q}^{(l,r)}(\cdot)$ used by the transmitter of the moment. Therefore, Eve has to select a mapping pattern $\mathfrak{S}_E^{(l,r)}(\cdot) = \mathfrak{F}_E^{(l)}(\cdot) \otimes \mathfrak{M}_E^{(l,r)}(\cdot)$ on her own for each data stream, and uses this pattern to perform MPA detection for obtaining the detected symbol probabilities of (12), $w = \mathfrak{F}_E^{(l)}(\mathbf{x}_a^{(l)}) | \mathfrak{M}_E^{(l,r)}(\mathbf{x}_d^{(l)}) \in \mathfrak{S}_E^{(l,r)}(\cdot)$, where $\mathfrak{F}_E^{(l)}(\cdot)$ and $\mathfrak{M}_E^{(l,r)}(\cdot)$ are Eve's selected SM and SCMA mapping patterns for the l^{th} data stream conveyed by the r^{th} subcarrier, respectively.

Therefore, even if Eve adopts the brute-force approach to search all PQ SM-SCMA mapping patterns, she has no basis for picking up the correct one used in the desired link and only has an equal probability of $1/(PQ)$ to guess the secret

key. This ensures that the confidential information delivered through the route in the AANET is protected from the attacks of third parties. Note that even if multiple eavesdroppers exist, each individual eavesdropper detects the received signal based on the CQI she obtained and still has a probability of $1/PQ$ to successfully select the correct secret key.

IV. SECRECY RATE IN AANET

In this section, we analyse the secrecy rate achieved by the CQI-mapped SM-SCMA scheme in multi-hop AANETs, which is defined as the positive difference between the achievable data rates obtained by the legitimate link and the wiretapping link, given finite-alphabet channel inputs.

As the 4×6 sparse spreading codebook of [46] is used, there are 3 data streams conveyed by each subcarrier. In each hop associated with a given channel realisation, the overall achievable data rate of the 6 streams conveyed by 4 subcarriers over the desired link with the inputs illustrated in Fig. 3 is given in (16), where the $N \times 1$ vector $\mathbf{d}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{k_1, k'_1, k_2, k'_2, k_3, k'_3(r)} = (\mathbf{h}_{m_1}^{(r)} s_{k_1}^{(r)} - \mathbf{h}_{m'_1}^{(r)} s_{k'_1}^{(r)}) + (\mathbf{h}_{m_2}^{(r)} s_{k_2}^{(r)} - \mathbf{h}_{m'_2}^{(r)} s_{k'_2}^{(r)}) + (\mathbf{h}_{m_3}^{(r)} s_{k_3}^{(r)} - \mathbf{h}_{m'_3}^{(r)} s_{k'_3}^{(r)})$ pertains to the r^{th} subcarrier associated with the transmitted signals $s_{k_i}^{(r)}, s_{k'_i}^{(r)} \in \mathfrak{M}_q^{(l,r)}(\cdot)$, $l \in \{l_1^{(r)}, l_2^{(r)}, l_3^{(r)}\}$, and $(m'_i, k'_i) \neq (m_i, k_i)$ excludes the event when $m'_i = m_i$ and $k'_i = k_i$ occur together from the summation, $i = 1, 2, 3$. Moreover, $\rho = 1/\sigma_Z^2$ is the unit-energy signal-to-noise power ratio (SNR), and $\mathcal{E}_z\{\cdot\}$ represents the expectation with respect to the AWGN received by the desired receiver within the r^{th} subcarrier, i.e. \mathbf{z}_r .

Apparently, as ρ tends to infinity, we have the achievable data rate of the desired wiretap channel in the noise-free scenario, expressed as

$$\lim_{\rho \rightarrow +\infty} C_D(\rho) = 6 \log_2(MK). \quad (17)$$

This gives the upper bound on the data rate of each hop with M TAs and K APM constellation points adopted by a SM-SCMA transmitter in the AANET simultaneously transmitting 6 data streams. For example, when we have $M = 4$ transmit antennas (TAs) and each of the $L = 6$ data streams adopts $K = 4$ -ary APM, we have a maximum data rate of 24 bits/sec/Hz.

On the other hand, the eavesdropper does not know the SM-SCMA mapping patterns in the desired link. Therefore, the achievable data rate for Eve in a given hop can be expressed as

$$C_E = 6 \left(\frac{1}{M} C_{Ea} + \frac{1}{K^3} C_{Ed} \right), \quad (18)$$

where $\frac{1}{M}$ indicates the right TA mapping patterns among the M candidates for Eve, while $\frac{1}{K^3}$ represents the correct mapping pattern among the K^3 available ones. Additionally, in (18), C_{Ea} and C_{Ed} denote the achievable data rates of the TA index bits $\mathbf{x}_a^{(l)}$ and the classic radiated bits $\mathbf{x}_d^{(l)}$ of the l^{th} data stream accessing Eve, respectively, if Eve could successfully decode them [25]. The expressions of C_{Ea} and C_{Ed} are given in (19) and (20), respectively. Therein, the $N_E \times 1$ vectors $\mathbf{q}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{(r)} = (\mathbf{g}_{m_1}^{(r)} - \mathbf{g}_{m'_1}^{(r)}) s_{k_1}^{(r)} + (\mathbf{g}_{m_2}^{(r)} -$

$$C_D = 6 \log_2(MK) - \frac{6}{4} \sum_{r=1}^4 \frac{1}{3M^3K^3} \sum_{m_1=1}^M \sum_{k_1=1}^K \sum_{m_2=1}^M \sum_{k_2=1}^K \sum_{m_3=1}^M \sum_{k_3=1}^K \mathcal{E}_z \left\{ \log_2 \left(1 + \sum_{\substack{m'_1=1 \\ (m'_1, k'_1) \neq (m_1, k_1)}}^M \sum_{k'_1=1}^K \sum_{\substack{m'_2=1 \\ (m'_2, k'_2) \neq (m_2, k_2)}}^M \sum_{k'_2=1}^K \right. \right. \\ \left. \left. \sum_{\substack{m'_3=1 \\ (m'_3, k'_3) \neq (m_3, k_3)}}^M \sum_{k'_3=1}^K \exp \left(-\rho \left[(\mathbf{d}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{k_1, k'_1, k_2, k'_2, k_3, k'_3(r)} + \mathbf{z}_r)^\dagger (\mathbf{d}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{k_1, k'_1, k_2, k'_2, k_3, k'_3(r)} + \mathbf{z}_r) - \mathbf{z}_r^\dagger \mathbf{z}_r \right] \right) \right) \right\} \quad (16)$$

$$C_{Ea} = \log_2 M - \frac{1}{4} \sum_{r=1}^4 \frac{1}{3M^3K^3} \sum_{m_1=1}^M \sum_{k_1=1}^K \sum_{m_2=1}^M \sum_{k_2=1}^K \sum_{m_3=1}^M \sum_{k_3=1}^K \mathcal{E}_z \left\{ \log_2 \left(\sum_{m'_1=1}^M \sum_{m'_2=1}^M \sum_{m'_3=1}^M \right. \right. \\ \left. \left. \exp \left(-\rho \left[(\mathbf{q}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{(r)} + \mathbf{z}_E^{(r)})^\dagger (\mathbf{q}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{(r)} + \mathbf{z}_E^{(r)}) - (\mathbf{z}_E^{(r)})^\dagger (\mathbf{z}_E^{(r)}) \right] \right) \right) \right\} \quad (19)$$

$$C_{Ed} = \log_2 K - \frac{1}{4} \sum_{r=1}^4 \frac{1}{3M^3K^3} \sum_{m_1=1}^M \sum_{k_1=1}^K \sum_{m_2=1}^M \sum_{k_2=1}^K \sum_{m_3=1}^M \sum_{k_3=1}^K \mathcal{E}_z \left\{ \log_2 \left(\sum_{m'_1=1}^M \sum_{k'_1=1}^K \sum_{m'_2=1}^M \sum_{k'_2=1}^K \right. \right. \\ \left. \left. \sum_{m'_3=1}^M \sum_{k'_3=1}^K \exp \left(-\rho \left(\mathbf{q}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{k_1, k'_1, k_2, k'_2, k_3, k'_3(r)} + \mathbf{z}_E^{(r)} \right)^\dagger \left(\mathbf{q}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{k_1, k'_1, k_2, k'_2, k_3, k'_3(r)} + \mathbf{z}_E^{(r)} \right) \right) \right) \right) \\ \left. - \log_2 \left(\sum_{m'_1=1}^M \sum_{m'_2=1}^M \sum_{m'_3=1}^M \exp \left(-\rho \left(\mathbf{q}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{(r)} + \mathbf{z}_E^{(r)} \right)^\dagger \left(\mathbf{q}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{(r)} + \mathbf{z}_E^{(r)} \right) \right) \right) \right\} \quad (20)$$

$\mathbf{g}_{m'_2}^{(r)} s_{k_2}^{(r)} + (\mathbf{g}_{m_3}^{(r)} - \mathbf{g}_{m'_3}^{(r)}) s_{k_3}^{(r)}$ and $\mathbf{q}_{m_1, m'_1, m_2, m'_2, m_3, m'_3}^{k_1, k'_1, k_2, k'_2, k_3, k'_3(r)} = (\mathbf{g}_{m_1}^{(r)} s_{k_1}^{(r)} - \mathbf{g}_{m'_1}^{(r)} s_{k'_1}^{(r)}) + (\mathbf{g}_{m_2}^{(r)} s_{k_2}^{(r)} - \mathbf{g}_{m'_2}^{(r)} s_{k'_2}^{(r)}) + (\mathbf{g}_{m_3}^{(r)} s_{k_3}^{(r)} - \mathbf{g}_{m'_3}^{(r)} s_{k'_3}^{(r)})$, where the transmitted signals $s_{k_i}^{(r)}, s_{k'_i}^{(r)} \in \mathfrak{M}_q^{(l, r)}(\cdot)$, $l \in \{l_1^{(r)}, l_2^{(r)}, l_3^{(r)}\}$, for $k_i, k'_i = 1, 2, \dots, K$, $m_i, m'_i = 1, 2, \dots, M$, $i = 1, 2, 3$. Moreover, $\mathcal{E}_z\{\cdot\}$ stands for the expectation with respect to the AWGN received by Eve in the r^{th} subcarrier, i.e., $\mathbf{z}_E^{(r)}$.

For a given channel realization, we have $\lim_{\rho \rightarrow +\infty} C_{Ea}(\rho) = \log_2 M$ and $\lim_{\rho \rightarrow +\infty} C_{Ed}(\rho) = \log_2 K$. As ρ goes to infinity, the limit of Eve's instantaneous data rate is obtained by

$$\lim_{\rho \rightarrow +\infty} C_E(\rho) = 6 \left(\frac{\log_2 M}{M} + \frac{\log_2 K}{K^3} \right). \quad (21)$$

For the AANET with T hops, the achievable end-to-end data rate of the CQI-mapped SM-SCMA in the routed path is given by

$$R_D^{(T)} = \min_{t=1, 2, \dots, T} \{C_{D,t}\}, \quad (22)$$

where $C_{D,t}$ is the overall data rate of the CQI-mapped SM-SCMA in the t^{th} hop, calculated through (16) using the channel realisation in the t^{th} hop of the routed path.

In the t^{th} hop, the data rate leaked to the third party can be expressed as

$$C_{E,t} = \min \left(C_{D,1}, C_{D,2}, \dots, C_{D,t-1}, C_E^{(t)} \right), \quad (23)$$

where $C_E^{(t)}$ is calculated through (18) using Eve's channel realisation in the t^{th} hop.

Subsequently, the data rate leaked in the T -hop AANET is

$$R_E^{(T)} = \max_{t=1, 2, \dots, T} \{C_{E,t}\}, \quad (24)$$

where $C_{E,t}$ is given by (23).

Now we can have the expression of the secrecy rate of a wiretap channel, which is the positive difference between the achievable data rates obtained by the legitimate link and the wiretapping link, i.e., if the legitimate link is better than the wiretapping link. For a T -hop AANET relying on our CQI-mapped SM-SCMA under study, the instantaneous secrecy rate is obtained by

$$R_s^{(T)} = \max(0, R_D^{(T)} - R_E^{(T)}), \quad (25)$$

where $R_D^{(T)}$ and $R_E^{(T)}$ are given by (22), and (24), respectively.

V. PERFORMANCE EVALUATION IN AANET

In this section, the security performance of the CQI-mapped SM-SCMA is evaluated within a multi-hop AANET, in terms of its BER in Section V-A and its ergodic secrecy rate in Section V-B. In the simulations, we employ the example parameters summarized in Table II for the AANET, where a Rician fading factor of $\kappa = 15$ dB is considered and the relative velocity between the transmitter and the receiver is 30 m/s.

A. BER Performance

To begin with, the end-to-end BER performance of the desired and the undesired receiver is investigated. Figs. 5 and 6

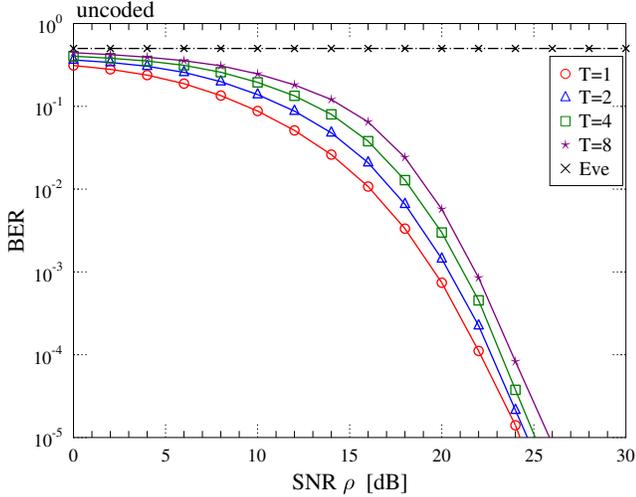
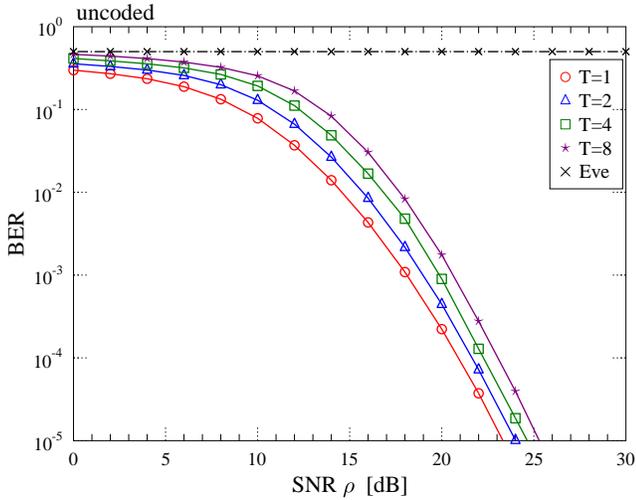
(a) $M = N = N_E = 2$ (b) $M = N = N_E = 4$

Fig. 5. Uncoded BER performance of the $T = 1, 2, 4, 8$ -hop AANET with a Rician fading factor of $\kappa = 15$ dB, where the CQI-mapped SM-SCMA employs $R = 4$ orthogonal subcarriers to support $L = 6$ data streams in the scenarios: (a) $M = N = N_E = 2$, and (b) $M = N = N_E = 4$, where the CQI-mapped SCMA and CQI-mapped MIMO-SCMA schemes are included as the benchmarks of our proposed CQI-mapped SM-SCMA.

demonstrate the uncoded and coded performance of the CQI-mapped SM-SCMA in multi-hop AANETs.

Figs. 5 (a) and (b) show the uncoded BER performance in the single-hop ($T = 1$) and multi-hop ($T = 2, 4, 8$) AANET employing $M = N = 2$ and $M = N = 4$ TAs, respectively, where the number of antennas at Eve is $N_E = 2$ and $N_E = 4$ as well. Given that a multi-hop AANET is considered, the number of RAs, N , is equal to that of the TAs, M , in each hop. Because the *detect-and-forward* technique is employed, the BER performance of the routed path degrades, as the number of hops increases. Specifically, a 2dB SNR loss can be observed from Fig. 5 (b) at the BER of 10^{-5} , when the number of hops in a AANET increases from $T = 1$ to $T = 8$. By contrast, since Eve cannot gain access to the CQI pattern of

the desired link in any hop, she is unable to identify the SM-SCMA mapping patterns activated by the secret key. Hence, Eve cannot detect the confidential information delivered over the routed path, relying on the MPA detection.

Additionally, by comparing Figs. 5 (a) and (b), we find that the BER performance of the routed path using $M = N = 4$ is around 1dB better than that of $M = N = 2$. This offers the insight that the tradeoff between the BER performance and the multi-antenna configuration cost has to be carefully considered in the practical design of AANETs. Moreover, the variance of the CQI $\gamma_m^{(r)} = (\mathbf{h}_m^{(r)})^\dagger (\mathbf{h}_m^{(r)})$ is given by $(6 - \frac{1}{2(\kappa+1)^2})N$, which is doubled when the number of RAs increases from $N = 2$ to $N = 4$, in any hop. From the PLS perspective of our CQI-mapped design, increasing the number of TAs, M , allows us to reduce the number of pilot symbols required for the high-probability identification of the active CQI pattern, mainly because the CQI falls within different confidence intervals at a similar probability. As such, the tradeoff between the resource utilisation efficiency and the multi-antenna configuration cost has to be taken into account for practical AANET designs.

Figs. 6 (a) and (b) further investigate the coded BER performance using the same parameters as Figs. 5 (a) and (b), respectively, where 1/2-rate turbo coding is employed. Herein, the *detect-and-forward* and *detect & decode-and-forward* techniques are compared for our multi-hop AANET. When *detect-and-forward* relaying is employed, the performance is degraded significantly upon increasing the number of hops, since only the MPA detection of the received signals is performed in the intermediate hops ($t = 1, \dots, T - 1$), while Log-BCJR turbo decoding is only performed in the last hop, i.e. at the T^{th} hop. For example, it can be observed from Fig. 6 (a) that doubling T from $T = 2$ to $T = 4$ leads to over 1dB performance degradation at a BER of 10^{-5} . By contrast, when the *detect & decode-and-forward* relaying is combined both with MPA detection and Log-BCJR turbo decoding, the performance loss is mitigated by at least 2.3dB, in the case of a AANET having $T = 2$ hops, as shown in Fig. 6 (a). However, this performance loss mitigation is achieved at the cost of a much higher computational complexity and latency, since the decoding cannot start until all the received symbols have been detected. We also remark that, for a single-hop AANET, there is no difference between these two approaches, where the MPA detection and the Log-BCJR turbo decoding are performed at the receiver, since the signals will not be forwarded.

When it comes to the performance of wiretapping links, Figs. 5 and 6 reveal that Eve's BER is always around 0.5, which implies that she cannot unveil any confidential information delivered over the routed path in the AANET relying on our CQI-mapped SM-SCMA, despite performing MPA detection and Log-BCJR turbo decoding as well. Hence, A2A communications in the routed path are secured by the proposed secret key.

Finally, for demonstrating the benefits of our proposed scheme, we compare our CQI-mapped SM-SCMA with several benchmark systems at the same transmission data rate of 6 bits per subcarrier (bps). Fig. 7 characterizes the uncoded BER performance of a single-hop ($T = 1$) AANET employing CQI-

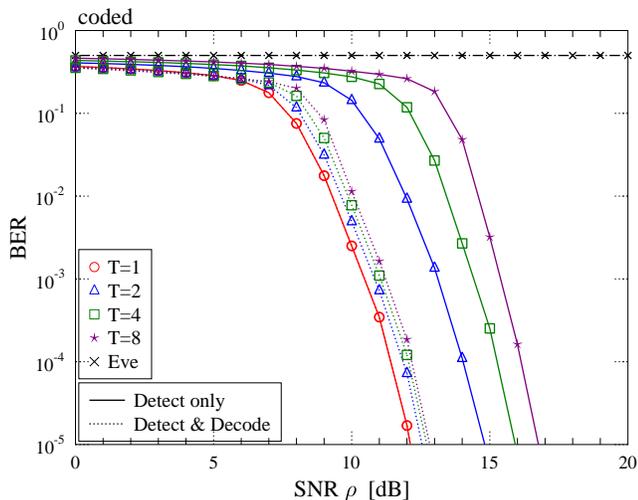
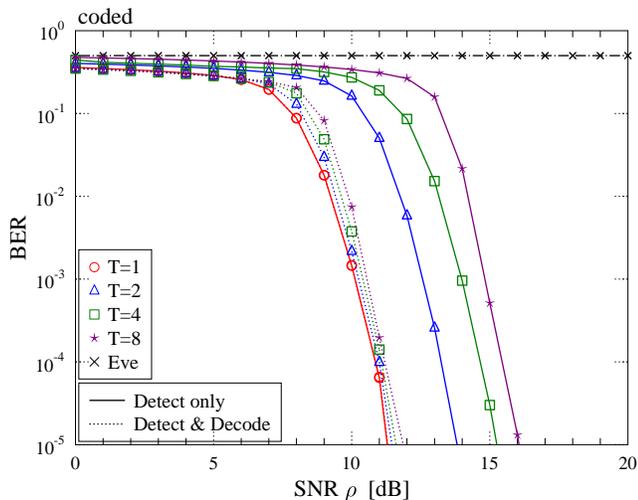
(a) $M = N = N_E = 2$ (b) $M = N = N_E = 4$

Fig. 6. Coded BER performance of the $T = 1, 2, 4, 8$ -hop AANET with a Rician fading factor of $\kappa = 15$ dB, where the 1/2-rate turbo-coded CQI-mapped SM-SCMA employs $R = 4$ orthogonal subcarriers to support $L = 6$ data streams in the scenarios: (a) $M = N = N_E = 2$, and (b) $M = N = N_E = 4$.

mapped SM-SCMA, SCMA, MIMO-SCMA and SM-OFDM using $N = 4$ RAs. As shown in Fig. 7, our CQI-mapped SM-SCMA employs $M = 4$ TAs and $K = 4$ -ary APM to transmit 4 bits by a single data stream. Since each data stream spreads over d_l subcarriers, each subcarrier in the 4×6 CQI-mapped SM-SCMA system transmits at 6 bps. By contrast, since SCMA employs only a single TA, $K = 16$ -ary APM has to be employed by each data stream, leading to the same rate of 6 bps, whereas $M = 4$ MIMO-SCMA only has to transmit 1 bit per TA per data stream. However, when each subcarrier transmits a single SM modulated symbol, SM-OFDM having $R = 4$ subcarriers supports up to $L = 4$ data streams. This leads to the choice of $M = 4$ and $K = 16$ for SM-OFDM. We can observe from Fig. 7 that our proposed CQI-mapped SM-SCMA exhibits the best BER performance among the four

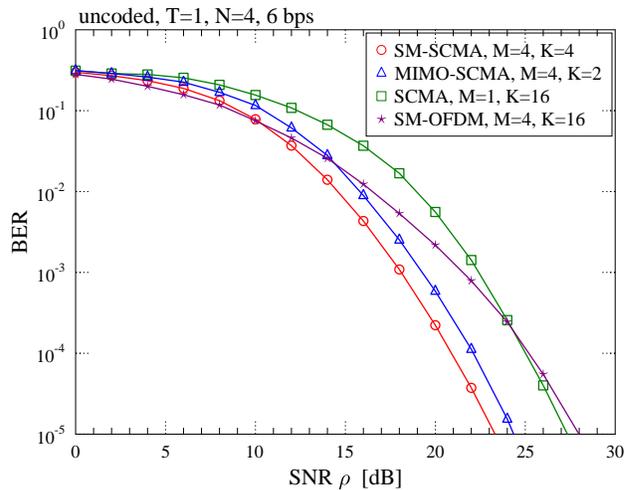


Fig. 7. Uncoded BER performance of the $T = 1$ -hop AANET with a Rician fading factor of $\kappa = 15$ dB employing CQI-mapped SM-SCMA, SCMA, MIMO-SCMA and SM-OFDM using $N = 4$, where the SCMA-related schemes employ $R = 4$ orthogonal subcarriers to support $L = 6$ data streams.

schemes, achieving at least 1dB SNR gain over MIMO-SCMA at a BER of 10^{-5} , which demonstrates the benefits of our design.

B. Ergodic secrecy rate

Next, we characterize the ergodic secrecy rate numerically based on the analysis of Section IV. Within the AANET, the desired and wiretapping links are independent and identically distributed (i.i.d.), and the channels exhibit frequency-selective fading, as given in (5) and (6), respectively.

In Fig. 8, the ergodic secrecy rate of a T -hop AANET using our CQI-mapped SM-SCMA, $\mathcal{E}\{R_s^{(T)}\}$, is plotted for the 4-point APM input illustrated in Fig. 3, where we have $K = 4$, $T = 1, 2, 4, 8$ and *detect & decode-and-forward* relaying is used. For the sake of comparison, the ergodic data rate of the routed path in the AANET, $\mathcal{E}\{R_D^{(T)}\}$, is also presented. As shown in this figure, both the data rate of the routed path and the secrecy rate decreases upon increasing the number of hops. However, the rate reduction is modest, particularly in Fig. 8 (b), because *detect & decode-and-forward* relaying experiences strong LoS propagation in the AANET, which mitigates the rate loss over multiple hops.

The ergodic data rate of the routed path in the AANET converges to 18 bits/sec/Hz in Fig. 8 (a) and 24 bits/sec/Hz in Fig. 8 (b), which agree with the limit in (17). Moreover, the ergodic secrecy rate converges to 14.8 bits/sec/Hz in Fig. 8 (a) and 20.8 bits/sec/Hz in Fig. 8 (b), which agrees with the limit given by

$$\begin{aligned} & \lim_{\rho \rightarrow +\infty} C_D(\rho) - C_E(\rho) \\ &= 6 \left(\frac{M-1}{M} \log_2 M + \frac{K^3-1}{K^3} \log_2 K \right). \end{aligned} \quad (26)$$

That is, the ergodic data rate leaked over the routed path in the AANET converges to 3.2 bits/sec/Hz for both cases of $M = 2$

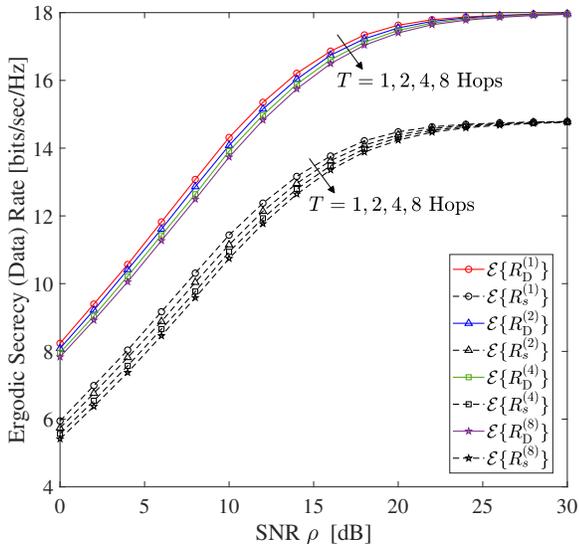
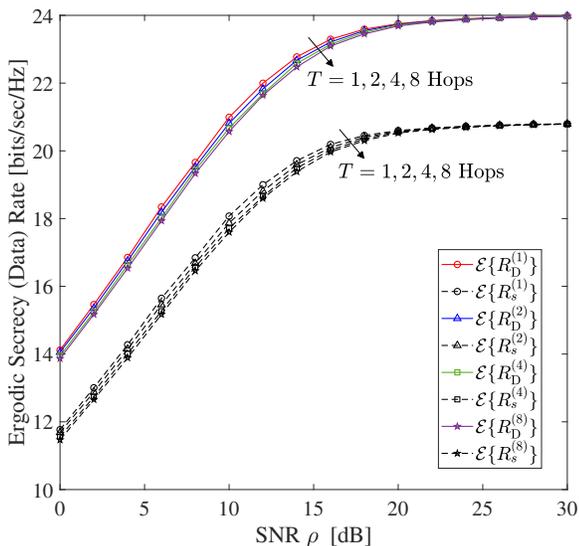
(a) $M = N = N_E = 2$ (b) $M = N = N_E = 4$

Fig. 8. Ergodic secrecy rate achieved by the T -hop AANET with CQI-mapped SM-SCMA of a 4-point APM input, $\mathcal{E}\{R_s^{(T)}\}$ for $T = 1, 2, 4, 8$ in the scenarios: (a) $M = N = N_E = 2$, and (b) $M = N = N_E = 4$. Also shown is the ergodic data rate of the routed path in the AANET, $\mathcal{E}\{R_D^{(T)}\}$, in these scenarios.

and $M = 4$ TAs with $K = 4$ APM, which agrees with the limit in (21).

C. Complexity

In this section, we quantify the detection complexity of our CQI-mapped SM-SCMA scheme when employing the state-of-the-art MPA detector, as discussed in Section III-A, in terms of the complexity order and the number of floating point operations (FLOPs) required by the MPA detector per iteration [47].

Specifically, when the optimal maximum-likelihood (ML) detector is adopted, the detector has to visit every possible

TABLE III
THE DETECTION COMPLEXITY OF THE MPA AND ML DETECTION FOR THE CQI-MAPPED SM-SCMA SYSTEM.

(M, N)	MPA ($\mathcal{O}[(KM)^{d_r}]$)	ML ($\mathcal{O}[(KM)^L]$)
(2, 2)	2.6×10^5	5.2×10^5
(4, 4)	3.9×10^5	6.7×10^7

symbol of all L data streams and each symbol transmitted by the l^{th} data stream is chosen out of KM candidates from $\mathfrak{S}_{p,q}^{(l,r)}(\cdot)$, giving a complexity order of $\mathcal{O}[(KM)^L]$ [31]. By contrast, the VN update of (9) dominates the complexity order of the MPA detector. Observe from (9) that the MPA algorithm deals with only d_r data streams sharing a single subcarrier, hence the number of multiplications is determined by the size of $\mathbf{x}_{[r]}$, which results in a complexity order of $\mathcal{O}[(KM)^{d_r}]$. When the MPA detector is employed for CQI-mapped SCMA or for CQI-mapped MIMO-SCMA, we have the complexity orders of $\mathcal{O}(K^{d_r})$ and $\mathcal{O}(K^{Md_r})$, respectively.

Furthermore, Table III quantifies the number of FLOPs required by the ML and MPA detector for our SM-SCMA system using $M = N = 2$ and $M = N = 4$, which shows that in contrast to the high-complexity ML detector, the MPA detector can be implemented in AANETs at an affordable complexity. Furthermore, a suite of sophisticated algorithms have been proposed in the literature [34], [35], which would further reduce the detection complexity of our proposed CQI-mapped SM-SCMA scheme.

VI. CONCLUSIONS

A CQI-mapped SM-SCMA scheme was conceived for improving the throughput while enhancing the PLS of multi-hop AANETs, which generates a secret key by activating a certain SM-SCMA mapping pattern based on the instantaneous CQI of the desired link in each hop. With this secret key in the multi-hop AANET, although the eavesdroppers have the opportunity to get multiple copies of the confidential messages that are being forwarded via the routed path, they are still unable to unveil the source information because they cannot access the CQI of desired links. Thus, they have no knowledge of the activated SM-SCMA mapping patterns. Moreover, the MPA detection and turbo coding were used for further improving the BER performance of the proposed scheme in the routed path of AANETs. Our BER performance and the ergodic secrecy rate results have substantiated that multi-hop AANETs using our proposed schemes, secure the desired A2A communications at high throughput.

Our future research will investigate other MIMO transmission approaches based on our CQI-varied mapping approach, providing promising candidates for future A2A secure communications.

REFERENCES

- [1] E. Haas, "Aeronautical channel modeling," *IEEE Transactions on Vehicular Technology*, vol. 51, no. 2, pp. 254–264, 2002.
- [2] X. Huang, J. A. Zhang, R. P. Liu, Y. J. Guo, and L. Hanzo, "Airplane-aided integrated networking for 6G wireless: Will it work?" *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 84–91, 2019.

- [3] D. Medina, F. Hoffmann, F. Rossetto, and C.-H. Rokitansky, "A geographic routing strategy for north atlantic in-flight Internet access via airborne mesh networking," *IEEE/ACM Transactions on Networking*, vol. 20, no. 4, pp. 1231–1244, 2011.
- [4] J. Zhang, S. Chen, R. G. Maunder, R. Zhang, and L. Hanzo, "Regularized zero-forcing precoding-aided adaptive coding and modulation for large-scale antenna array-based air-to-air communications," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 9, pp. 2087–2103, 2018.
- [5] J. Zhang, T. Chen, S. Zhong, J. Wang, W. Zhang, X. Zuo, R. G. Maunder, and L. Hanzo, "Aeronautical *ad hoc* networking for the Internet-above-the-clouds," *Proceedings of the IEEE*, vol. 107, no. 5, pp. 868–911, 2019.
- [6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016.
- [7] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.
- [8] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.
- [9] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3532–3545, 2012.
- [10] F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao, and G. Qian, "Robust beamforming for physical layer security in BDMA massive MIMO," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 775–787, 2018.
- [11] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2007–2020, 2013.
- [12] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.
- [13] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 682–694, 2013.
- [14] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219–228, 2017.
- [15] Z. Kong, S. Yang, D. Wang, and L. Hanzo, "Robust beamforming and jamming for enhancing the physical layer security of full duplex radios," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3151–3159, 2019.
- [16] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, 2011.
- [17] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.
- [18] A. Bilzhaue, B. Belgacem, M. Mostafa, and T. Graupl, "DataLink security in the l-band digital aeronautical communications system (LDACS) for air traffic management," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 11, pp. 22–33, 2017.
- [19] M. Sajatovic, B. Haindl, M. Ehammer, T. Gräupl, M. Schnell, U. Epple, and S. Brandes, "LDACS1 system definition proposal," *Eurocontrol Study, Edition*, vol. 1, 2009.
- [20] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2016.
- [21] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 467–471, 2015.
- [22] F. Wu, W. Wang, C. Dong, and L. Yang, "Performance analysis of secret precoding-aided spatial modulation with finite-alphabet signaling," *IEEE Access*, vol. 6, pp. 29 366–29 381, 2018.
- [23] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1351–1354, 2015.
- [24] G. Xia, F. Shu, Y. Zhang, J. Wang, S. ten Brink, and J. Speidel, "Antenna selection method of maximizing secrecy rate for green secure spatial modulation," *IEEE Transactions on Green Communications and Networking*, vol. 3, no. 2, pp. 288–301, 2019.
- [25] Y. Yang and M. Guizani, "Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 877–889, 2018.
- [26] J. Zhang, S. Chen, R. G. Maunder, R. Zhang, and L. Hanzo, "Adaptive coding and modulation for large-scale antenna array-based aeronautical communications in the presence of co-channel interference," *IEEE Transactions on Wireless Communications*, vol. 17, no. 2, pp. 1343–1357, 2017.
- [27] C. Xu, J. Zhang, T. Bai, P. Botsinis, R. G. Maunder, R. Zhang, and L. Hanzo, "Adaptive coherent/non-coherent single/multiple-antenna aided channel coded ground-to-air aeronautical communication," *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1099–1116, 2018.
- [28] Y. Liu, Z. Qin, M. ElKashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Non-orthogonal multiple access for 5G and beyond," *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2347–2381, 2017.
- [29] X. Wang, J. Wang, L. He, and J. Song, "Spectral efficiency analysis for downlink NOMA aided spatial modulation with finite alphabet inputs," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 562–10 566, 2017.
- [30] Y. Liu, L.-L. Yang, and L. Hanzo, "Spatial modulation aided sparse code-division multiple access," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1474–1487, 2018.
- [31] Y. Liu, L.-L. Yang, P. Xiao, H. Haas, and L. Hanzo, "Spatial modulated multicarrier sparse code-division multiple access," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 610–623, 2020.
- [32] Y. Liu, L.-L. Yang, and L. Hanzo, "Sparse space-time-frequency-domain spreading for large-scale non-orthogonal multiple access," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12 327–12 332, 2020.
- [33] H. Nikopour and H. Baligh, "Sparse code multiple access," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2013, pp. 332–336.
- [34] I. Al-Nahhal, O. A. Dobre, E. Basar, and S. Ikki, "Low-cost uplink sparse code multiple access for spatial modulation," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9313–9317, 2019.
- [35] I. Al-Nahhal, O. A. Dobre, and S. Ikki, "On the complexity reduction of uplink sparse code multiple access for spatial modulation," *IEEE Transactions on Communications*, vol. 68, no. 11, pp. 6962–6974, 2020.
- [36] Y. Chen, L. Wang, Y. Ai, B. Jiao, and L. Hanzo, "Performance analysis of NOMA-SM in vehicle-to-vehicle massive MIMO channels," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 12, pp. 2653–2666, 2017.
- [37] S. Abdel-Razeq, S. Zhou, R. Bansal, and M. Zhao, "Uplink NOMA transmissions in a cooperative relay network based on statistical channel state information," *IET Communications*, vol. 13, no. 4, pp. 371–378, 2018.
- [38] M. Jain, N. Sharma, A. Gupta, D. Rawal, and P. Garg, "Performance analysis of NOMA assisted mobile *ad hoc* networks for sustainable future radio access," *IEEE Transactions on Sustainable Computing*, 2020.
- [39] Y. Liu, Z. Qin, M. ElKashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.
- [40] B. He, A. Liu, N. Yang, and V. K. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2196–2206, 2017.
- [41] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1670–1683, 2018.
- [42] Z. Xiang, W. Yang, Y. Cai, Z. Ding, and Y. Song, "Secure transmission design in HARQ assisted cognitive NOMA networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2528–2541, 2020.
- [43] M. Sajatovic, B. Haindl, U. Epple, T. Gräupl, C. Rihacek, M. Schnell, N. Fistas, J. Koch, H. Kim, and E. Le-Ho, "Updated LDACS1 system specification," *SESAR Joint Undertaking Report EWA04-1-T2-D1*, 2011.
- [44] P. Yang, Y. Xiao, B. Zhang, M. El-Hajjar, S. Li, and L. Hanzo, "Phase rotation-based precoding for spatial modulation systems," *IET Communications*, vol. 9, no. 10, pp. 1315–1323, 2015.
- [45] L. Hanzo, T. Liew, B. Yeap, R. Tee, and S. X. Ng, *Turbo coding, turbo equalisation and space-time coding: EXIT-chart-aided near-capacity designs for wireless channels*. John Wiley & Sons, 2011.

- [46] M. Taherzadeh, H. Nikopour, A. Bayesteh, and H. Baligh, "SCMA codebook design," in *2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*, 2014, pp. 1–5.
- [47] Z. Tang, J. Wang, J. Wang, and J. Song, "A low-complexity detection algorithm for uplink NOMA system based on Gaussian approximation," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2017, pp. 1–6.