Physical-Layer Secret Key Generation via CQI-Mapped Spatial Modulation in Multi-Hop Wiretap Ad-Hoc Networks

Yuli Yang, Meng Ma, Sonia Aïssa, Lajos Hanzo

***Abstract*— Providing security guarantee is a critical concern in the *ad-hoc* networks relying on multi-hop channels, since their flexible topology is vulnerable to security attacks. To enhance the security of a spatial modulation (SM) assisted wireless network, various SM mapping patterns are activated by random channel quality indicator (CQI) patterns over the legitimate link, as a physical-layer secret key. The SM signals are encrypted by random mapping patterns to prevent eavesdroppers from correctly demapping their detections. This secret key is developed for multi-hop wiretap *ad-hoc* networks, where eavesdroppers might monitor all the transmitting nodes of a legitimate link. We substantially characterise the multi-hop wiretap model with receiver diversity techniques adopted by eavesdroppers. The security performance of the conceived scheme is evaluated in the scenarios where eavesdroppers attempt to detect their received signals using maximal-ratio combining or maximum-gain selection. The achievable data rates of both legitimate and wiretapper links are formulated with the objective of quantifying the secrecy rates for both Gaussian-distributed and finite-alphabet inputs. Illustrative numerical results are provided for the metrics of ergodic secrecy rate and secrecy outage probability, which substantiate the compelling benefits of the physical-layer secret key generation via CQI-mapped SM.**

***Index Terms*— Ad-hoc networks, channel quality indicator (CQI), multi-hop, multiple-input-multiple-output (MIMO) wiretap channel, physical layer security (PLS), secrecy rate, spatial modulation (SM).**

I. Introduction

In contrast to traditional network security techniques that reckon on higher-layer encryption, physical layer security (PLS) exploits the inherent randomness of wireless channels for secret key generation to prevent any eavesdropper (Eve) from extracting confidential information by wiretapping [1]–[3]. Therefore, PLS is particularly suitable for the low-complexity devices and the dynamically fluctuating topology of *ad-hoc* networks, such as the Internet-of-things (IoT), where higher-layer encryption cannot be readily implemented without the infrastructure [4]–[6].

Early PLS studies are initiated from an information-theoretic perspective [7]–[9], where wiretapper links are deemed to be degraded versions of legitimate links. To turn non-degraded wiretapper links into degraded ones, PLS can be realised by inflicting extra interference upon Eve, specifically through security-oriented beamforming or precoding [10]–[12], jamming [13]–[15], and artificial noise [16]–[18]. Moreover, cooperative signal processing and relay selection protocols are advanced for PLS improvement [19], [20]. Then, the information-theoretic secret key is exchanged over a legitimate link based on the physical-layer attribute differences between the degraded wiretapper link and the legitimate link [21], [22]. These PLS techniques exploit the random characteristics of wireless channels in conjunction with multi-antenna configurations, typically stipulating the idealised assumption that Eve's channel state information (CSI) or its statistics is available at the legitimate transmitter.

An attractive multi-antenna solution is spatial modulation (SM) [23]–[26], which has been exploited for enhancing the PLS through a random data-driven selection of transmit antennas (TAs) governed by the information bits mapped onto the TAs and the legitimate user's CSI. In particular, precoding or artificial-noise aided SM is developed to minimize Eve's received power while maximising the legitimate receiver's power [27]. Jamming or beamforming aided SM is developed for transmitting the interference to Eve in the null-space of the legitimate receiver [28], [29]. Furthermore, relay selection is developed for SM in dual-hop cooperative networks to achieve PLS [30].

Against this backdrop, we aim to exploit the random characteristics of information sources rather than those of channel states to generate a physical-layer secret key and boost the security. More specifically, the secret key is generated by varying the SM mapping patterns, i.e., the bit-to-symbol mapping and the TA selection. In [31], an adaptive bit-to-symbol mapper was designed for SM to optimise the bit error rate (BER), with an extremely high complexity in the computation and comparison of the BERs pertaining to all possible mapping patterns. To reduce the complexity, near-optimal solutions can be identified at the receiver and their index may be signalled back to the transmitter through a feedback channel [32]. Unfortunately, this feedback provides Eve with more opportunities to monitor the SM mapping patterns adopted in the legitimate link. As a design alternative,

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

M. Ma is with the School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China (e-mail: mam@pku.edu.cn).

S. Aïssa is with the Institut National de la Recherche Scientifique (INRS), University of Quebec, Montreal, QC H5A 1K6, Canada (e-mail: aissa@emt.inrs.ca).

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

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/N004558/1, EP/P034284/1, EP/P034284/1, EP/P003990/1 (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
CONTRASTING THE NOVELTY OF OUR WORK TO THE LITERATURE.

Contributions	Ours	[5]	[7], [8], [12] [14]–[18], [22]	[9]–[11], [13] [19]–[21]	[27]–[29]	[30]	[31] [32]	[33]	[34]	[35]	[36]	[37]
Physical Layer Security	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
Spatial Modulation	✓				✓	✓	✓	✓	✓	✓		
Bit-to-Symbol Mapping	✓						✓			✓		
TA Selection	✓							✓	✓	✓		✓
Relaying	✓	✓		✓		✓						
Multi-Hop	✓	✓										
MRC at Eve	✓										✓	✓
MGS at Eve	✓											

Euclidean-distance based TA selection was designed for SM in [33], [34] but, again, the exhaustive search over all possible TA selection patterns leads to an excessive complexity. Anyhow, the adaptive bit-to-symbol mapping and the optimised TA selection unveil the possibility to address a moderate level of PLS. To degrade Eve's decoding performance for the purpose of enhancing the PLS, a physical-layer secret key was also generated by activating various SM mapping patterns on the basis of the legitimate channel quality indicator (CQI) [35]. The complexity of this secret key generation is relatively low, because *(i)* the CSI of the links spanning from legitimate transmitters to Eve is not involved at all, *(ii)* the CQI over a legitimate link is known at the transmitter and desired receiver readily and synchronously in the time division duplex (TDD) mode, and *(iii)* the active SM mapping pattern is selected in a straightforward way, without complicated computation.

Compared to conventional wireless networks, it is more challenging for *ad-hoc* and IoT networks to achieve the requirements on high flexibility and low complexity in the PLS implementation. Motivated by this, we further develop the physical-layer secret key generation via CQI-mapped SM for multi-hop wiretap *ad-hoc* networks and quantify its performance. Since a SM signal is forwarded several times over a multi-hop wiretap channel, Eve has multiple opportunities to detect the information. Given the availability of multiple copies of the SM signal received from the legitimate link, receiver diversity techniques can be exploited by Eve for enhancing her detection performance via maximal-ratio combining (MRC) or maximum-gain selection (MGS). The average secrecy capacity and/or the secrecy outage probability of a point-to-point link have been evaluated for the scenarios where Eve adopts multi-antenna MRC [36] and TA selection [37] to enhance the chance of her successful detection. Concerning the vulnerability of multi-hop *ad-hoc* networks, in this paper we investigate the scenarios where Eve distributes multi-antenna frontends to monitor all legitimate nodes' transmissions. In particular, Eve adopts multi-hop MRC or multi-hop MGS to process the multiple signal copies she has received from the legitimate link. In these scenarios, we formulate the achievable data rates of both the legitimate link and the wiretapper link as well as the secrecy rates of multi-hop wiretap *ad-hoc* networks, under the assumptions of both Gaussian-distributed inputs and realistic finite-alphabet inputs in the SM mapping for the physical-layer secret key generation.

The novel contributions of this work are contrasted to the literate of PLS and/or SM in Table I. Specifically, our main contributions are three-fold:

- To improve the security of *ad-hoc* and IoT networks, the CQI-mapped SM is exploited for the physical-layer secret key generation in the context of multi-hop multiple-input-multiple-output (MIMO) wiretap channels, where none of the legitimate nodes knows the CSI of the links spanning from themselves to Eve.
- We completely characterise the multi-hop wiretap *ad-hoc* networks where Eve benefits from distributed multi-antenna frontends to collect multiple copies of the SM signal forwarded over the legitimate link and employs multi-hop MRC and multi-hop MGS for boosting her detection capability.
- The mathematical framework of both the secrecy rates and their outage probabilities achieved by multi-hop wiretap *ad-hoc* networks relying on the proposed physical-layer secret key is established in the characterised scenarios with both Gaussian-distributed and finite-alphabet inputs.

To detail the aforementioned contributions, the remainder of this paper is organized as follows. Firstly, the developed physical-layer secret key for a multi-hop MIMO wiretap *ad-hoc* network and its BER performance are presented in Section II. Subsequently, the achievable data rates of both the legitimate link and the wiretapper link are analysed in Sections III and IV, respectively, where both Gaussian-distributed and finite-alphabet inputs are investigated, when Eve relies on MRC or MGS. Based on this mathematical framework, Section V analyses the secrecy rates of the considered multi-hop wiretap *ad-hoc* networks and provides numerical results. Finally, we conclude 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 $\mathbf{I}_M$ is the $M \times M$ identity matrix. The conjugate, the transpose, the conjugate transpose and the modulus operators are represented by $(\cdot)^*$, $(\cdot)^{\mathrm{T}}$, $(\cdot)^\dagger$ and $|\cdot|$, respectively. Moreover, $d^2(u,v)$ denotes the squared Euclidean distance between signals u and v, and $\max(0,x)$ is the maximum value between 0 and x. The

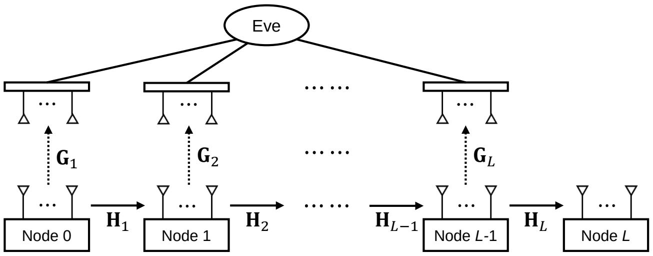


Fig. 1. The model of a multi-hop MIMO wiretap *ad-hoc* network, where Eve distributes multi-antenna frontends to collect multiple copies of the signal forwarded over the legitimate link.

factorial of a positive integer M is denoted by $M!$, i.e., $M! = M \times (M-1) \times \cdots \times 2 \times 1$. In addition, $\mathscr{E}\{\cdot\}$ represents the expectation (mean) operator and $\Pr\{\cdot\}$ stands for the probability of an event. The probability density function (PDF) of a random variable x is denoted by $p(x)$, and the conditional PDF of x given the event of $y = A$ is denoted by $p(x|y = A)$.

II. Network Model and Secret Key Generation

In this section, the physical-layer secret key generation via CQI-mapped SM is developed for multi-hop MIMO wiretap *ad-hoc* networks.

A. Network Model

The network model is shown in Fig. 1, where the legitimate link is composed of $L+1$ nodes, and hence we have L hops. The communication between the source, denoted by Node 0, and the destination, i.e., Node L, needs $L-1$ intermediate nodes' assistance. The number of antennas at Node l is M_l, where $l = 0, 1, \cdots, L$. Due to the constraints on radio module and battery life of *ad-hoc* and IoT devices, the legitimate nodes have to transmit their signals at a low power, which guarantees ignorable interference received at undesired nodes over the legitimate link as well as negligible amount of information leaked to eavesdroppers. Thus, the number of hops in the legitimate link is determined by the distance from the source to the destination and the transmit power of each intermediate node.

To improve the resource utilisation efficiency, the TDD mode is exploited in each hop, which allows multiple nodes in an *ad-hoc* network to access a shared spectral band and hence no wasteful guard bands are needed. Moreover, the channel reciprocity of the TDD mode allows a pair of communicating nodes to exploit each other's CSI without using a feedback channel. More specifically, the CSI of the link spanning from Node $l-1$ to Node l is the same as that from Node l to Node $l-1$ and vice versa. Therefore, Node $l-1$ can exploit the CSI of the link spanning from itself to Node l by using Node l's pilot symbols to estimate the CSI of the link spanning from Node l to itself.

Consider the confidential information delivered from Node 0 to Node L, via $L-1$ intermediate nodes' forwarding. In the multi-hop *ad-hoc* network under study, Eve is assumed to have a sophisticated receiver, which allows us to investigate the maximum possible information leakage. More explicitly, to maximise Eve's wiretapping capability in the interest of quantifying the maximum possible information leakage, we assume that she has L frontends, each relying on N_{E} antennas, for monitoring all legitimate nodes' transmissions in their vicinity. In other words, Eve is able to collect the signals transmitted by all the L hops and exploits all these signals to unveil the confidential information conveyed over the legitimate link. We note that this wiretapper link model is utilised for theoretically quantifying the maximum information leakage, which is equivalent to Eve's achievable data rate through the most powerful wiretapping. In practice, an eavesdropper might not be readily capable of obtaining the signals from all the hops over the legitimate link, especially not when the number of hops is very large. Hence in a nutshell, we quantify the multi-hop *ad-hoc* network security guaranteed by our proposed design in the absolute worst-case scenario of Eve having the most powerful wiretapping capability.

In the legitimate link, the channel of the l^{th} hop, spanning from Node $l-1$ to Node l, is characterised by the $M_l \times M_{l-1}$ matrix $\mathbf{H}_l = [h_{nm}^{(l)}]_{M_l \times M_{l-1}} = [\mathbf{h}_1^{(l)}, \mathbf{h}_2^{(l)}, \cdots, \mathbf{h}_{M_{l-1}}^{(l)}]$, where the $M_l \times 1$ vector $\mathbf{h}_m^{(l)} = [h_{1m}^{(l)}, h_{2m}^{(l)}, \cdots, h_{M_l,m}^{(l)}]^{\mathrm{T}}$ contains the channel coefficients from the m^{th} antenna of Node $l-1$ to all the antennas of Node l, for $l \in \{1, 2, \cdots, L\}$, $m = 1, 2, \cdots, M_{l-1}$, $n = 1, 2, \cdots, M_l$.

As for the wiretapper link, the channels spanning from Node $l-1$ to Eve's frontend that monitors this node are represented by the $N_{\mathrm{E}} \times M_{l-1}$ matrices $\mathbf{G}_l = [g_{nm}^{(l)}]_{N_{\mathrm{E}} \times M_{l-1}} = [\mathbf{g}_1^{(l)}, \mathbf{g}_2^{(l)}, \cdots, \mathbf{g}_{M_{l-1}}^{(l)}]$, where $l = 1, 2, \cdots, L$, $m = 1, 2, \cdots, M_{l-1}$, $n = 1, 2, \cdots, N_{\mathrm{E}}$, and the $N_{\mathrm{E}} \times 1$ vector $\mathbf{g}_m^{(l)} = [g_{1m}^{(l)}, g_{2m}^{(l)}, \cdots, g_{N_{\mathrm{E}},m}^{(l)}]^{\mathrm{T}}$ contains the channel coefficients from the m^{th} antenna of Node $l-1$ to all the antennas of the frontend monitoring Node $l-1$.

Herein, the legitimate and wiretapper links are independent and identically distributed (i.i.d.) flat-fading over the same spectrum band, and all the channels' coefficients are assumed to obey i.i.d. complex Gaussian distributions, i.e., $h_{nm}^{(l)}, g_{nm}^{(l)} \sim \mathcal{CN}(0, 1)$, $\forall\ l \in \{1, 2, \cdots, L\}$, $m \in \{1, 2, \cdots, M_{l-1}\}$, $n \in \{1, 2, \cdots, M_l, N_{\mathrm{E}}\}$.

B. Secret Key Generation

Since the CSI is not transmitted in the TDD mode for the handshaking between the communicating nodes, eavesdroppers cannot access the legitimate CSI through wiretapping. As such, the generation of physical-layer secret key in this work relies on the instantaneous CQI pattern in each hop.

In the majority of previous contributions, the CSI knowledge is directly exploited for enhancing the level of PLS by beamforming, precoding, jamming or artificial noise; see [10]–[22], [27]–[30] and the references therein. The objective of these PLS techniques is to degrade wiretapper links, while improving the legitimate link quality. An important assumption in these schemes is that the transmitter knows the wiretapper link's CSI or at least its statistics, which are then exploited for beamforming, precoding, jamming or artificial noise generation. However, this assumption is impractical, especially when the eavesdroppers are non-authorised subscribers. Furthermore, the eavesdroppers typically do not transmit. Hence,

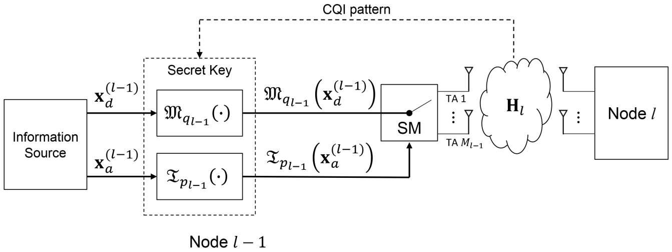

CQI pattern
Secret Key
Information Source
$\mathbf{x}_d^{(l-1)}$
$\mathbf{x}_a^{(l-1)}$
$\mathfrak{M}_{q_{l-1}}(\cdot)$
$\mathfrak{T}_{p_{l-1}}(\cdot)$
$\mathfrak{M}_{q_{l-1}}\left(\mathbf{x}_d^{(l-1)}\right)$
$\mathfrak{T}_{p_{l-1}}\left(\mathbf{x}_a^{(l-1)}\right)$
SM
TA 1
TA M_{l-1}
$\mathbf{H}_l$
Node l
Node $l-1$

Fig. 2. The physical-layer secret key generation via CQI-mapped SM for the l^{th} hop in the channel $\mathbf{H}_l$ over the legitimate link.

estimating their CSI is rather unfeasible and only best-case results can be attained. To dispense this idealized simplifying assumption, we use the SM mapping pattern as a secret key, which is governed by the random instantaneous CQI of the legitimate link.

In the l^{th} hop's channel $\mathbf{H}_l$, the CQI of TA m at Node $l-1$ to all the antennas at Node l is denoted by $\gamma_m^{(l)} = (\mathbf{h}_m^{(l)})^\dagger(\mathbf{h}_m^{(l)})$, where $l \in \{1, 2, \cdots, L\}$ and $m \in \{1, 2, \cdots, M_{l-1}\}$; thus, the CQI pattern in this hop is the permutation containing all $\gamma_m^{(l)}$ in descending or ascending order.

For example, if Node $l-1$ has $M_l = 2$ TAs, there are two CQI patterns in the l^{th} hop, i.e., Pattern 1 is $\gamma_1^{(l)} > \gamma_2^{(l)}$ and Pattern 2 is $\gamma_2^{(l)} > \gamma_1^{(l)}$. When $M_l = 4$, there are 24 permutations of the 4 CQIs, $\gamma_1^{(l)}$, $\gamma_2^{(l)}$, $\gamma_3^{(l)}$, $\gamma_4^{(l)}$, in the l^{th} hop, i.e., $\gamma_1^{(l)} > \gamma_2^{(l)} > \gamma_3^{(l)} > \gamma_4^{(l)}$, $\gamma_4^{(l)} > \gamma_3^{(l)} > \gamma_2^{(l)} > \gamma_1^{(l)}$, and so on. From an ergodic view point, the total number of CQI patterns in the l^{th} hop is $P_{l-1} = M_{l-1}!$ and these patterns occur at the same probability.

The physical-layer secret key generation via CQI-mapped SM in the l^{th} hop of the legitimate link is presented in Fig. 2, where the transmitter Node $l-1$ formats its SM mapping patterns based on the instantaneous CQI pattern of this hop's channel $\mathbf{H}_l$, as a secret key to enhance the PLS, $l \in \{1, 2, \cdots, L\}$.

The initial source information at Node 0 is denoted by $\mathbf{x}_0 = [\mathbf{x}_a^{(0)}, \mathbf{x}_d^{(0)}]$ and the decode-and-forward protocol is applied in the legitimate link. Without loss of generality, the source information bit stream in the l^{th} hop is expressed as $\mathbf{x}_{l-1} = [\mathbf{x}_a^{(l-1)}, \mathbf{x}_d^{(l-1)}]$, where the vectors $\mathbf{x}_a^{(l-1)}$ and $\mathbf{x}_d^{(l-1)}$ contain the TA information bits and the classic amplitude/phase-shift keying (APSK) information bits, respectively, to be conveyed by Node $l-1$. The number of APSK-mapping patterns at Node $l-1$ is $Q_{l-1} = K_{l-1}!$, where K_{l-1} is the number of APSK constellation points adopted by Node $l-1$. Moreover, since Node $l-1$ has M_{l-1} antennas, the number of TA-index patterns is equal to the number of CQI patterns in the channel $\mathbf{H}_l$, $P_{l-1} = M_{l-1}!$.

More specifically, the varied SM mapping patterns are deemed to be the physical-layer secret keys in each hop of the legitimate link. That is, the APSK-mapping patterns and TA-index patterns are varied according to instantaneous CQI patterns over the legitimate link.

In an arbitrary transmission, if the $p_{l-1}{}^{\mathrm{th}}$ CQI pattern occurs in the l^{th} hop channel $\mathbf{H}_l$, Node $l-1$ will exploit the $p_{l-1}{}^{\mathrm{th}}$ TA-index pattern, denoted by $\mathfrak{T}_{p_{l-1}}(\cdot)$, $p_{l-1} \in \{1, 2, \cdots, P_{l-1}\}$, and the $q_{l-1}{}^{\mathrm{th}}$ APSK-mapping pattern pertaining to the CQI pattern of this signalling interval also termed as channel-use, denoted by $\mathfrak{M}_{q_{l-1}}(\cdot)$, $q_{l-1} \in \{1, 2, \cdots, Q_{l-1}\}$. In this hop, the received baseband signals at Node l and Eve are formulated as

$$\mathbf{y}_{\mathrm{D},l} = \mathbf{h}^{(l)}_{\mathfrak{T}_{p_{l-1}}(\mathbf{x}_a^{(l-1)})} \mathfrak{M}_{q_{l-1}}(\mathbf{x}_d^{(l-1)}) + \mathbf{z}_{\mathrm{D},l} \tag{1}$$

and

$$\mathbf{y}_{\mathrm{E},l} = \mathbf{g}^{(l)}_{\mathfrak{T}_{p_{l-1}}(\mathbf{x}_a^{(l-1)})} \mathfrak{M}_{q_{l-1}}(\mathbf{x}_d^{(l-1)}) + \mathbf{z}_{\mathrm{E},l}, \tag{2}$$

respectively, where the $M_l \times 1$ vectors $\mathbf{y}_{\mathrm{D},l}$ and $\mathbf{z}_{\mathrm{D},l} \sim \mathcal{CN}\left(\mathbf{0}_{M_l \times 1}, \sigma_W^2 \mathbf{I}_{M_l}\right)$ contain Node l's received signals and the additive white Gaussian noise (AWGN) components, respectively. Meanwhile, the $N_{\mathrm{E}} \times 1$ vectors $\mathbf{y}_{\mathrm{E},l}$ and $\mathbf{z}_{\mathrm{E},l} \sim \mathcal{CN}\left(\mathbf{0}_{N_{\mathrm{E}} \times 1}, \sigma_W^2 \mathbf{I}_{N_{\mathrm{E}}}\right)$ contain Eve's received signals and AWGN components, respectively, during the l^{th} hop in the legitimate link. Moreover, the subscript $\mathfrak{T}_{p_{l-1}}(\mathbf{x}_a^{(l-1)})$ denotes the TA index activated by $\mathbf{x}_a^{(l-1)}$ according to the $p_{l-1}{}^{\mathrm{th}}$ TA-index pattern at Node $l-1$. Therefore, the $M_l \times 1$ vector $\mathbf{h}^{(l)}_{\mathfrak{T}_{p_{l-1}}(\mathbf{x}_a^{(l-1)})}$ and the $N_{\mathrm{E}} \times 1$ vector $\mathbf{g}^{(l)}_{\mathfrak{T}_{p_{l-1}}(\mathbf{x}_a^{(l-1)})}$ contain the channels' coefficients spanning from the activated TA at Node $l-1$ to Node l and Eve's frontend that monitors Node $l-1$, respectively. In addition, $\mathfrak{M}_{q_{l-1}}(\mathbf{x}_d^{(l-1)})$ is the APSK input transmitted by Node $l-1$, which is mapped by $\mathbf{x}_d^{(l-1)}$ according to the $q_{l-1}{}^{\mathrm{th}}$ APSK-mapping pattern.

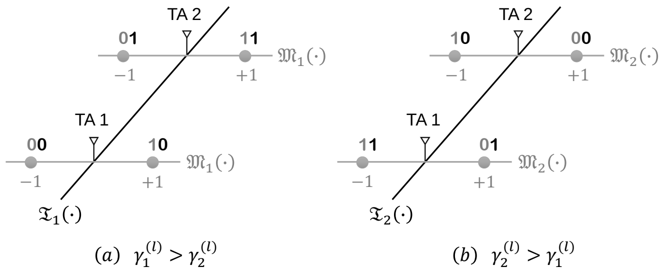
For instance, if Node $l-1$ has 2 TAs for conveying the TA information $\mathbf{x}_a^{(l-1)}$ and adopts BPSK modulation for transmitting the APSK information $\mathbf{x}_d^{(l-1)}$, there will be $P_{l-1} = 2$ TA-index patterns and $Q_{l-1} = 2$ APSK-mapping patterns. The physical-layer secret key generation in this case, i.e., the variation of SM mapping patterns based on the instantaneous CQI pattern, is illustrated in Fig. 3. When the first CQI pattern ($\gamma_1^{(l)} > \gamma_2^{(l)}$) occurs, the SM mapping patterns are given by Fig. 3 (a), where the first TA-index pattern $\mathfrak{T}_1(\cdot)$ and the first APSK-mapping pattern $\mathfrak{M}_1(\cdot)$ are activated. In detail, $\mathfrak{T}_1(0) = 1$, $\mathfrak{T}_1(1) = 2$, and $\mathfrak{M}_1(0) = -1$, $\mathfrak{M}_1(1) = +1$. When the second CQI pattern ($\gamma_2^{(l)} > \gamma_1^{(l)}$) occurs, the SM mapping patterns are given by Fig. 3 (b), where the second TA-index pattern $\mathfrak{T}_2(\cdot)$ and the second APSK-mapping pattern $\mathfrak{M}_2(\cdot)$ are activated. That is, $\mathfrak{T}_2(1) = 1$, $\mathfrak{T}_2(0) = 2$, and $\mathfrak{M}_2(1) = -1$, $\mathfrak{M}_2(0) = +1$. Since Eve is unable to access the CQI patterns of the legitimate link, she has no knowledge on the SM mapping patterns and, hence, does not have correct basis to demap the confidential information conveyed over the legitimate link.

III. Signal Detection

In this section, the signal detection methods in the legitimate link and the wiretapper link are detailed, based on which the simulation results of their BER performance are reported.

A. Detection in the Legitimate Link

Thanks to the channel reciprocity in TDD mode, Node l always knows the instantaneous CQI pattern in the channel $\mathbf{H}_l$ through CSI estimation. Accordingly, the APSK-mapping



(a) $\gamma_1^{(l)} > \gamma_2^{(l)}$ (b) $\gamma_2^{(l)} > \gamma_1^{(l)}$

Fig. 3. The physical-layer secret key generation via CQI-mapped SM with BPSK and 2 TAs in the l^{th} hop.

pattern $\mathfrak{M}_{q_{l-1}}(\cdot)$ and the TA-index pattern $\mathfrak{T}_{p_{l-1}}(\cdot)$ exploited by Node $l-1$ are also known to Node l.

Upon receiving the signals $\mathbf{y}_{\mathrm{D},l}$, Node l may detect the APSK information $\mathbf{x}_d^{(l-1)}$ and the TA information $\mathbf{x}_a^{(l-1)}$ according to the following twin-step maximum-likelihood algorithm [24]: Firstly, the candidate decisions are made in terms of

$$\mathfrak{M}_{q_{l-1}}(\hat{\mathbf{x}}_{d,m}^{(l-1)}) = \underset{s\in\mathfrak{M}_{q_{l-1}}(\cdot)}{\arg\min}\ d^2\left(s, \frac{(\mathbf{h}_m^{(l)})^{\dagger}\mathbf{y}_{\mathrm{D},l}}{(\mathbf{h}_m^{(l)})^{\dagger}(\mathbf{h}_m^{(l)})}\right), \qquad m=1,2,\cdots,M_{l-1}; \tag{3}$$

and then, Node l will choose $\hat{\mathbf{x}}_d^{(l-1)} = \hat{\mathbf{x}}^{(l-1)}_{d,\mathfrak{T}_{p_{l-1}}(\hat{\mathbf{x}}_a^{(l-1)})}$ while getting $\hat{\mathbf{x}}_a^{(l-1)}$ if and only if

$$\mathfrak{T}_{p_{l-1}}(\hat{\mathbf{x}}_a^{(l-1)}) = \underset{m\in\{1,2,\cdots,M_{l-1}\}}{\arg\min}\ d^2\left(\mathfrak{M}_{q_{l-1}}(\hat{\mathbf{x}}_{d,m}^{(l-1)}), \frac{(\mathbf{h}_m^{(l)})^{\dagger}\mathbf{y}_{\mathrm{D},l}}{(\mathbf{h}_m^{(l)})^{\dagger}(\mathbf{h}_m^{(l)})}\right). \tag{4}$$

After detecting the information transmitted from Node $l-1$ in the l^{th} hop, Node l will forward its detected information, $\hat{\mathbf{x}}_d^{(l-1)}$ and $\hat{\mathbf{x}}_a^{(l-1)}$, to Node $l+1$ in the $l+1^{\mathrm{th}}$ hop. Hence, the APSK information and the TA information to be transmitted from Node l are $\mathbf{x}_d^{(l)} = \hat{\mathbf{x}}_d^{(l-1)}$ and $\mathbf{x}_a^{(l)} = \hat{\mathbf{x}}_a^{(l-1)}$, respectively.

As such, the physical-layer secret key generation via CQI-mapped SM is activated for each hop of the legitimate link, and the L^{th} hop is the last one, where the destination Node L gets the source information $\hat{\mathbf{x}}_d^{(L-1)}$ and $\hat{\mathbf{x}}_a^{(L-1)}$ by detecting the signals transmitted from Node $L-1$.

B. Detection in the Wiretapper Link

Eve will attempt to detect the source information $\mathbf{x}_0$ based on her own received signals, $\mathbf{y}_{\mathrm{E},l}$, $l=1,2,\cdots,L$, by wiretapping all hops of the legitimate link. However, since Eve does not know the CQI pattern in any hop of the legitimate link, she has no information on the physical-layer secret key, i.e., the SM mapping patterns $\mathfrak{M}_{q_{l-1}}(\cdot)$ and $\mathfrak{T}_{p_{l-1}}(\cdot)$, generated in the legitimate hops, $l=1,2,\cdots,L$. Therefore, Eve will reckon on her anticipated APSK-mapping pattern $\mathfrak{M}_{\mathrm{E},l-1}(\cdot)$ and TA-index pattern $\mathfrak{T}_{\mathrm{E},l-1}(\cdot)$ to demap the source information in the l^{th} hop.

Since Eve has collected L versions of the source information from the L hops, she will attain diversity gains using the following two methods.

1) Maximal-Ratio Combining (MRC): Eve's decision on the source information $\hat{\mathbf{x}}_0$ is made using the maximum-likelihood algorithm of

$$\hat{\mathbf{x}}_0 = \underset{\mathbf{s}_0}{\arg\min}\sum_{l=1}^{L} d^2\left(\mathbf{y}_{\mathrm{E},l},\ \mathbf{g}^{(l)}_{\mathfrak{T}_{\mathrm{E},l-1}(\mathbf{s}_a^{(l-1)})}\mathfrak{M}_{\mathrm{E},l-1}(\mathbf{s}_d^{(l-1)})\right), \tag{5}$$

where the bit stream $\mathbf{s}_0$ is divided into two streams $\mathbf{s}_a^{(l-1)}$ and $\mathbf{s}_d^{(l-1)}$ with respect to the l^{th} hop in the legitimate link. The lengths of $\mathbf{s}_a^{(l-1)}$ and $\mathbf{s}_d^{(l-1)}$ are determined by the number of TAs at Node $l-1$, M_{l-1}, and the number of APSK constellation points adopted by Node $l-1$, K_{l-1}, respectively.

2) Maximum-Gain Selection (MGS): Eve will process the signals received through the maximum-gain wiretapping channel $\mathbf{G}_{l^*}$ to make her final decision on the source information $\hat{\mathbf{x}}_0 = [\hat{\mathbf{x}}_a^{(0)}, \hat{\mathbf{x}}_d^{(0)}]$, where we have

$$l^* = \underset{l\in\{1,2,\cdots,L\}}{\arg\max}\ \frac{1}{M_{l-1}}\sum_{m=1}^{M_{l-1}} (\mathbf{g}_m^{(l)})^{\dagger}(\mathbf{g}_m^{(l)}). \tag{6}$$

In detail, Eve's candidate decisions on the APSK input transmitted by Node l^*-1 are made in terms of

$$\mathfrak{M}_{\mathrm{E},l^*-1}(\hat{\mathbf{x}}_{d,m}^{(0)}) = \underset{s\in\mathfrak{M}_{\mathrm{E},l^*-1}(\cdot)}{\arg\min}\ d^2\left(s, \frac{(\mathbf{g}_m^{(l^*)})^{\dagger}\mathbf{y}_{\mathrm{E},l^*}}{(\mathbf{g}_m^{(l^*)})^{\dagger}(\mathbf{g}_m^{(l^*)})}\right), \qquad m=1,2,\cdots,M_{l^*-1}; \tag{7}$$

and subsequently, Eve will choose $\hat{\mathbf{x}}_d^{(0)} = \hat{\mathbf{x}}^{(0)}_{d,\mathfrak{T}_{\mathrm{E},l^*-1}(\hat{\mathbf{x}}_a^{(0)})}$, while making a decision concerning the activated TA index in terms of

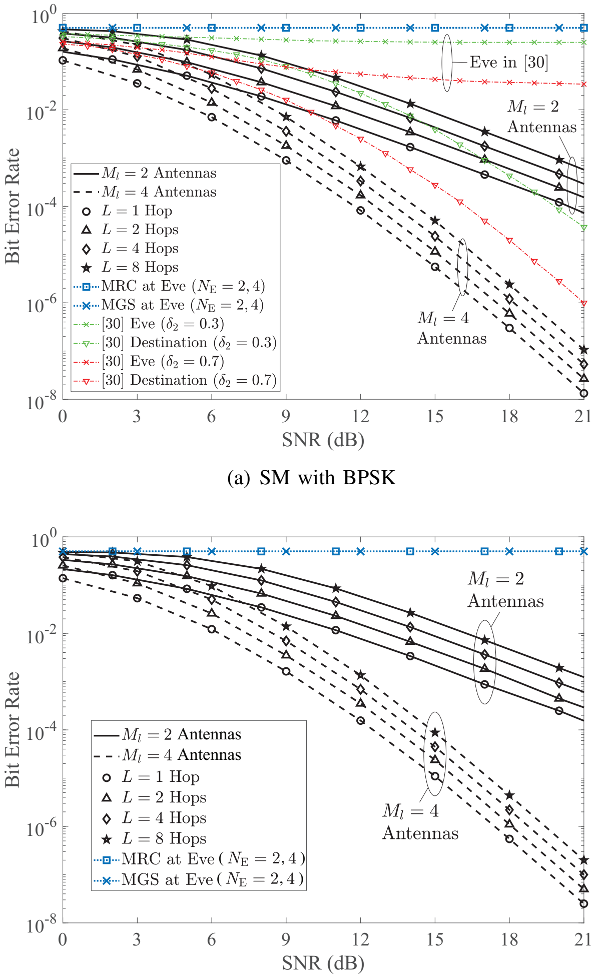
$$\mathfrak{T}_{\mathrm{E},l^*-1}(\hat{\mathbf{x}}_a^{(0)}) = \underset{m\in\{1,2,\cdots,M_{l^*-1}\}}{\arg\min}\ d^2\left(\mathfrak{M}_{\mathrm{E},l^*-1}(\hat{\mathbf{x}}_{d,m}^{(0)}), \frac{(\mathbf{g}_m^{(l^*)})^{\dagger}\mathbf{y}_{\mathrm{E},l^*}}{(\mathbf{g}_m^{(l^*)})^{\dagger}(\mathbf{g}_m^{(l^*)})}\right). \tag{8}$$

Although both these receive-diversity techniques may help Eve to improve her detection performance of the SM signals forwarded over the legitimate link, she still cannot obtain the correct APSK information $\mathbf{x}_d^{(0)}$ and/or TA information $\mathbf{x}_a^{(0)}$, because she is unaware of the SM mapping patterns utilised. Even if Eve could use a brute-force approach to search all possible SM mapping patterns, she has no basis to pick up the correct one. Hence, the secrecy of the confidential messages conveyed over the legitimate link will be guaranteed by the physical-layer secret key.

C. Bit Error Rate

Herein, the BER performance of multi-hop *ad-hoc* networks with the proposed secret key generation via CQI-mapped SM is investigated in the following two scenarios.

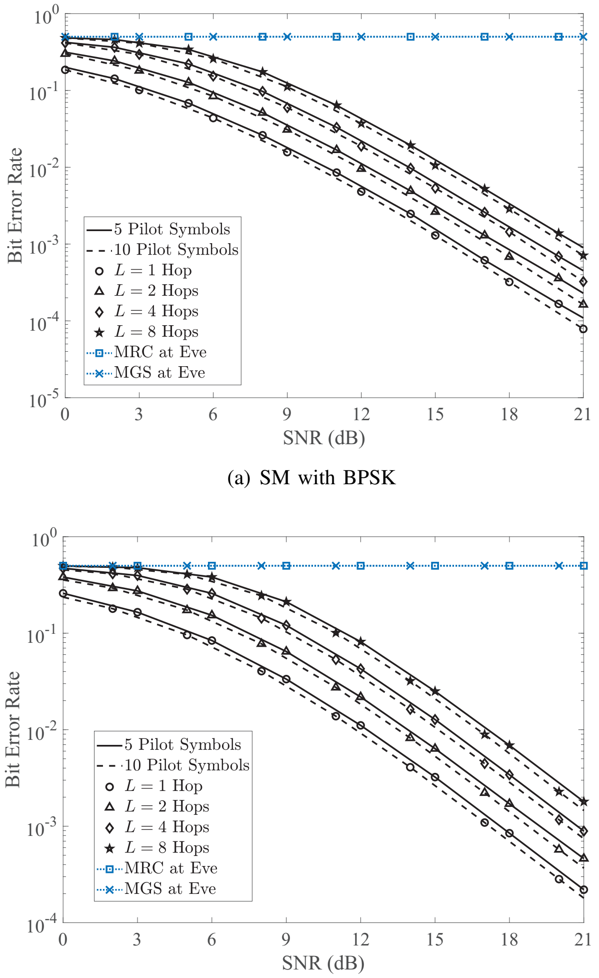
1) Perfect CSI/CQI at the Transmitter and Receiver in Each Hop: For this scenario, the BER comparisons between single-hop ($L=1$) and multi-hop ($L=2,4,8$) wiretap *ad-hoc* networks with our proposed secret key generation design are reported in Fig. 4, where the number of antennas set at each legitimate node, $M_l=2$ and 4. Eve's BER is also presented, with $N_{\mathrm{E}}=2$ and 4 antennas at each wiretapping frontend.



(a) SM with BPSK

(b) SM with QPSK

Fig. 4. BER of $L = 1, 2, 4, 8$-hop *ad-hoc* networks using the secret key generation via CQI-mapped SM in the scenario of perfect CSI known with $M_l = 2, 4$. Eve's BER with perfect CSI, $N_{\rm E} = 2, 4$, is also shown for comparison.



(a) SM with BPSK

(b) SM with QPSK

Fig. 5. BER of $L = 1, 2, 4, 8$-hop *ad-hoc* networks using the secret key generation via CQI-mapped SM in the scenario of practical channel estimation with 5 and 10 pilot symbols, $M_l = 2$. Eve's BER with perfect CSI, $N_{\rm E} = 2$, is also shown for comparison.

This figure reveals that the BER performance of the legitimate link gets worse with the increase in the number of hops and gets better with the increase in the number of antennas set at each node.

A further observation in this figure is that, with the proposed design, Eve cannot obtain any information forwarded over the legitimate link, regardless of how many antennas at each wiretapping frontend using whether MRC or MGS, if our secret key generation is adopted by legitimate nodes. The main reason behind this is that the legitimate CQI pattern is unavailable to Eve and, thus, Eve has no basis of choosing correct SM mapping patterns to demap her detection.

In addition, the BER performance of the destination and Eve in [30] is provided in Fig. 4(a) for the sake of comparison, where jamming with relay selection is exploited to implement the PLS in a dual-hop ($L = 2$) network with precoded SM. In this network, the source has $M_0 = 4$ TAs, each relay has 2 antennas, the destination has 4 antennas, and Eve has 4 antennas as well. It is assumed that Eve's CSI is perfectly known by the legitimate link for the jamming. Moreover, the transmit power is divided into two parts, i.e., δ_l for the SM precoding and $(1 - \delta_l)$ for the jamming, $l = 1, 2$. The power allocation for SM precoding is $\delta_1 = 0.5$ in the first hop, and $\delta = 0.3, 0.7$ in the second hop. As is shown in this figure, both the destination and Eve achieve better performance when more power is used for the SM precoding, namely less power for the jamming. Compared to this scheme, our proposed design has two main merits: higher energy efficiency and lower information leakage. Firstly, we do not need extra transmit power to jam Eve; thereby, all the transmit power contributes to the legitimate SM transmission. Secondly, Eve's BER performance is always around 0.5 in our scheme, regardless of how she detects her received signals, since she cannot correctly demap the confidential information.

2) Practical Channel Estimation at the Transmitter and Receiver in Each Hop: The BER performance of $L = 1, 2, 4, 8$-hop *ad-hoc* networks with our proposed physical-layer secret key generation in this scenario is presented in Fig. 5, where the CSI estimations using 5 pilot symbols and 10 pilot symbols are investigated for the case of $M_l = 2$ antennas set at each

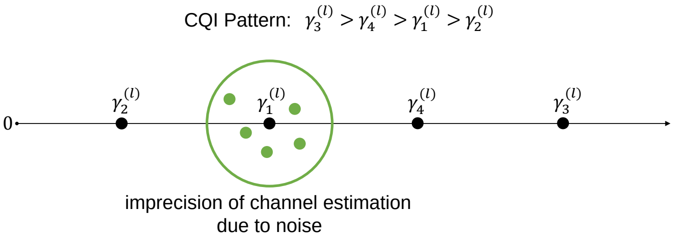

CQI Pattern: $\gamma_3^{(l)} > \gamma_4^{(l)} > \gamma_1^{(l)} > \gamma_2^{(l)}$
0
$\gamma_2^{(l)}$
$\gamma_1^{(l)}$
$\gamma_4^{(l)}$
$\gamma_3^{(l)}$
imprecision of channel estimation due to noise

Fig. 6. The impact of channel estimation imprecision on the accuracy of CQI pattern recognition.

legitimate node. Moreover, Eve's BER is also provided, with $N_{\mathrm{E}} = 2$ antennas at each wiretapping frontend. As is shown in this figure, better channel estimation, i.e., using more pilot symbols, leads to better BER performance of the legitimate link. Comparing the case of $M_l = 2$ antennas in Figs. 4 and 5, we may find that the BER difference between the scenarios of perfect CSI and channel estimation using 10 pilot symbols is negligible, specifically in the region of high signal-to-noise power ratio (SNR).

From the perspective of channel estimation, the channel estimation error is equivalent to the induction of extra noise and the perfect CSI can be achieved by using more pilot symbols or increasing transmit power in the channel estimation. Furthermore, the CQI in the l^{th} hop, $\gamma_m^{(l)} = \left(\mathbf{h}_m^{(l)}\right)^{\dagger}(\mathbf{h}_m^{(l)})$, is a random variable with mean M_l and variance $5.5M_l$. Given that the variance increases linearly with the number of receive antennas, M_l, each CQI value is expected to become more equi-probable upon increasing the number of receive antennas in the l^{th} hop. Hence, the system is more likely to correctly recognize the active CQI pattern for a high number of receive antennas, which improves the PLS. By contrast, the channel estimation accuracy has a lower impact on the PLS.

For example, the impact of channel estimation imprecision on the accuracy of CQI pattern recognition is shown in Fig. 6, for the l^{th} hop with $M_{l-1} = 4$ TAs, where the CQI pattern of the moment is $\gamma_3^{(l)} > \gamma_4^{(l)} > \gamma_1^{(l)} > \gamma_2^{(l)}$. The impact of the channel estimation imprecision due to noise is denoted by the green circle, whose radius is reduced through using more pilot symbols or increasing transmit power in the channel estimation. On the other hand, setting more receive antennas enlarges the distance between CQIs at higher probability. Therefore, the imprecision of channel estimation will have no influence on the accuracy of CQI pattern recognition and the legitimate link performance, if sufficient pilot symbols and receive antennas are utilised in each hop.

As such, we will study the multi-hop *ad-hoc* network security rate achieved by our proposed design in the scenario of perfect CSI known by both the legitimate link and the wiretapper link.

IV. Achievable Data Rate of the Legitimate Link

To evaluate the security performance of the proposed secret key generation in multi-hop wiretap *ad-hoc* networks, from an information-theoretic perspective, the achievable data rate of the legitimate link is firstly formulated in this section. Then, the secrecy rate will be obtained by comparing the achievable data rate of the legitimate link and Eve's achievable data rate that is formulated in next section.

A. Gaussian-Distributed Input

The achievable data rates of Gaussian-distributed inputs represent the upper bounds of realistic finite-alphabet inputs. Explicitly, the signals transmitted from all nodes over the legitimate link are restricted to be the random variables chosen from complex Gaussian distributed codebooks $\mathcal{CN}(0, \sigma_X^2)$ at the transmit power of σ_X^2. Hence, in this subsection we refer to Gaussian information instead of APSK information.

In the multi-hop MIMO wiretap *ad-hoc* network using our proposed secret key, the instantaneous data rate of the legitimate link having Gaussian-distributed inputs can be expressed as

$$C_{\mathrm{D}} = \min\left(C_{\mathrm{D}}^{(1)}, C_{\mathrm{D}}^{(2)}, \cdots, C_{\mathrm{D}}^{(L)}\right), \tag{9}$$

where $C_{\mathrm{D}}^{(l)}$ is the instantaneous data rate in the l^{th} hop, $l = 1, 2, \cdots, L$, obtained by

$$C_{\mathrm{D}}^{(l)} = C_{\mathrm{D}a}^{(l)} + C_{\mathrm{D}d}^{(l)}, \tag{10}$$

with $C_{\mathrm{D}a}^{(l)}$ and $C_{\mathrm{D}d}^{(l)}$ denoting the achievable data rates pertaining to SM transmissions of the TA information $\mathbf{x}_a^{(l-1)}$ and the Gaussian information $\mathbf{x}_d^{(l-1)}$, respectively, from Node $l-1$ to Node l.

In detail, the term $C_{\mathrm{D}a}^{(l)}$ in (10) is calculated using

$$\begin{aligned} C_{\mathrm{D}a}^{(l)} = \frac{1}{M_{l-1}} \sum_{m=1}^{M_{l-1}} \int_{\bar{y}_{\mathrm{D},l}} & p\left(\bar{y}_{\mathrm{D},l} | \mathbf{x}_a^{(l-1)}\right) \\ & \times \log_2 \frac{p\left(\bar{y}_{\mathrm{D},l} | \mathbf{x}_a^{(l-1)}\right)}{p(\bar{y}_{\mathrm{D},l})} d\bar{y}_{\mathrm{D},l}, \end{aligned} \tag{11}$$

where $\bar{y}_{\mathrm{D},l} = (\mathbf{h}_m^{(l)})^{\dagger}\mathbf{y}_{\mathrm{D},l}$ is the signal detected by Node l, as shown in (3) and (4). As the input $\mathfrak{M}_{q_{l-1}}(\mathbf{x}_d^{(l-1)})$ is complex Gaussian distributed, the conditional PDF of $\bar{y}_{\mathrm{D},l}$ given the TA information $\mathbf{x}_a^{(l-1)}$ is formulated as

$$p\left(\bar{y}_{\mathrm{D},l} | \mathbf{x}_a^{(l-1)}\right) = \frac{1}{\pi\sigma_{\bar{y}_{\mathrm{D},l}}^2} \exp\left(-\frac{|\bar{y}_{\mathrm{D},l}|^2}{\sigma_{\bar{y}_{\mathrm{D},l}}^2}\right), \tag{12}$$

where $\sigma_{\bar{y}_{\mathrm{D},l}}^2 = [(\mathbf{h}_m^{(l)})^{\dagger}(\mathbf{h}_m^{(l)})]^2\sigma_X^2 + (\mathbf{h}_m^{(l)})^{\dagger}(\mathbf{h}_m^{(l)})\sigma_W^2$ is the variance of $\bar{y}_{\mathrm{D},l}$ with respect to the Gaussian-distributed input $\mathfrak{M}_{q_{l-1}}(\mathbf{x}_d^{(l-1)})$ transmitted from the m^{th} TA at Node $l-1$. Accordingly, the PDF of $\bar{y}_{\mathrm{D},l}$ is obtained in the form of

$$p(\bar{y}_{\mathrm{D},l}) = \frac{1}{M_{l-1}} \sum_{m=1}^{M_{l-1}} p\left(\bar{y}_{\mathrm{D},l} | \mathbf{x}_a^{(l-1)}\right). \tag{13}$$

Additionally, the second item on the right-hand side of (10), $C_{\mathrm{D}d}^{(l)}$, is given by

$$C_{\mathrm{D}d}^{(l)} = \frac{1}{M_{l-1}} \sum_{m=1}^{M_{l-1}} \log_2\left(1 + \frac{\sigma_X^2}{\sigma_W^2}(\mathbf{h}_m^{(l)})^{\dagger}(\mathbf{h}_m^{(l)})\right). \tag{14}$$

By substituting (11) and (14) into (10), the instantaneous data rate for the transmission of confidential SM messages in the l^{th} hop over the legitimate link, i.e. from Node $l-1$ to

Node l, is accomplished. Subsequently, the legitimate link rate in the case of Gaussian-distributed input given by (9) will be obtained.

B. Finite-Alphabet Input

The transmit power of each node is denoted by σ_X^2 and the resultant SNR is $\rho = \sigma_X^2/\sigma_W^2$. The instantaneous data rate of the legitimate link with finite-alphabet inputs is expressed as

$$R_{\mathrm{D}} = \min\left(R_{\mathrm{D}}^{(1)}, R_{\mathrm{D}}^{(2)}, \cdots, R_{\mathrm{D}}^{(L)}\right). \tag{15}$$

Herein, the instantaneous data rate in the l^{th} hop, dented by $R_{\mathrm{D}}^{(l)}$, $l = 1, 2, \cdots, L$, is formulated by (16), where the $M_l \times 1$ vector $\mathbf{d}_{m,m'}^{(l)k,k'} = \mathbf{h}_m^{(l)} s_k^{(l)} - \mathbf{h}_{m'}^{(l)} s_{k'}^{(l)}$ associated with $s_k^{(l)}, s_{k'}^{(l)} \in \mathfrak{M}_{q_{l-1}}(\cdot)$, and $(m', k') \neq (m, k)$ excludes the event when $m' = m$ and $k' = k$ occur together from the summation. Moreover, $\mathscr{E}_z\{\cdot\}$ represents the expectation with respect to the AWGN received at Node l, i.e., $\mathbf{z}_{\mathrm{D},l}$ in (1).

As shown in (16), for a given channel realization, $f(\rho)$ is a monotonically decreasing function of the SNR ρ and converges to 1, when ρ tends to infinity, i.e., $\lim_{\rho \to +\infty} f(\rho) = 1$. Thus, as ρ approaches infinity, we have the limit of

$$\lim_{\rho \to +\infty} R_{\mathrm{D}}^{(l)}(\rho) = \log_2(M_{l-1} K_{l-1}), \tag{17}$$

which is the upper bound on the data rate of the l^{th} hop having M_{l-1} TAs and K_{l-1} APSK constellation points adopted by Node $l-1$.

V. Achievable Data Rate in the Wiretapper Link

In this section, Eve's achievable data rates are analysed for both Gaussian-distributed and finite-alphabet inputs in multi-hop MIMO wiretap *ad-hoc* networks exploiting the CQI-mapped SM. Since Eve may detect the source information $\mathbf{x}_0$ using MRC (5) or MGS (7)–(8), we will formulate her achievable data rates in these two scenarios.

A. Maximal-Ratio Combining (MRC)

In this scenario, Eve's instantaneous data rate is expressed as

$$C_{\mathrm{E,MRC}} = \min\left(C_{\mathrm{D}}^{(1)}, C_{\mathrm{D}}^{(2)}, \cdots, C_{\mathrm{D}}^{(L-1)}, C_{\mathrm{E}}^{(L)}\right) \tag{18}$$

for Gaussian-distributed inputs, and as

$$R_{\mathrm{E,MRC}} = \min\left(R_{\mathrm{D}}^{(1)}, R_{\mathrm{D}}^{(2)}, \cdots, R_{\mathrm{D}}^{(L-1)}, R_{\mathrm{E}}^{(L)}\right) \tag{19}$$

for finite-alphabet inputs. Herein, $C_{\mathrm{E}}^{(L)}$ and $R_{\mathrm{E}}^{(L)}$ denote Eve's achievable data rates, when using MRC to process the signals received from all nodes, i.e., Nodes $1, 2, \cdots, L-1$, for Gaussian-distributed and finite-alphabet inputs, respectively. Moreover, $C_{\mathrm{D}}^{(l)}$ and $R_{\mathrm{D}}^{(l)}$ are given by (10) and (16), respectively, for $l = 1, 2, \cdots, L-1$.

1) Gaussian-Distributed Input: The number of Gaussian-distributed constellation points at each node, K_{l-1}, $l = 1, 2, \cdots, L$, is infinite and, consequently, the probability that Eve can successfully demap the Gaussian-distributed input $\mathfrak{M}_{q_{l-1}}(\mathbf{x}_d^{(l-1)})$ transmitted by Node $l-1$ is 0, if the bit-to-symbol mapping pattern is varied in each channel-use. Hence, Eve's achievable data rate when using MRC is given by

$$C_{\mathrm{E}}^{(L)} = \frac{1}{L} \sum_{l=1}^{L} \frac{1}{M_{l-1}} C_{\mathrm{E}a}^{(l)}, \tag{20}$$

where $C_{\mathrm{E}a}^{(l)}$ is the data rate gleaned from the TA-index detection by Eve in the l^{th} hop, provided that she could successfully demap $\mathbf{x}_a^{(l-1)}$. Elaborating a little further, we have

$$\begin{aligned} C_{\mathrm{E}a}^{(l)} = \frac{1}{M_{l-1}} \sum_{m=1}^{M_{l-1}} \int_{\mathbf{y}_{\mathrm{E},l}} & p\left(\mathbf{y}_{\mathrm{E},l} | \mathbf{x}_a^{(l-1)}\right) \\ & \times \log_2 \frac{p\left(\mathbf{y}_{\mathrm{E},l} | \mathbf{x}_a^{(l-1)}\right)}{p(\mathbf{y}_{\mathrm{E},l})} d\mathbf{y}_{\mathrm{E},l}, \end{aligned} \tag{21}$$

where $\mathbf{y}_{\mathrm{E},l}$ is the signal received by Eve in the l^{th} hop, given in (2). Since the input $\mathfrak{M}_{q_{l-1}}(\mathbf{x}_d^{(l-1)})$ is complex Gaussian distributed, the conditional PDF of $\mathbf{y}_{\mathrm{E},l}$ given the TA information $\mathbf{x}_a^{(l-1)}$ is denoted by

$$p\left(\mathbf{y}_{\mathrm{E},l} | \mathbf{x}_a^{(l-1)}\right) = \frac{1}{\pi \sigma_{y_{\mathrm{E},l}}^2} \exp\left(-\frac{|\mathbf{y}_{\mathrm{E},l}|^2}{\sigma_{y_{\mathrm{E},l}}^2}\right), \tag{22}$$

where $\sigma_{y_{\mathrm{E},l}}^2 = (\mathbf{g}_m^{(l)})^\dagger (\mathbf{g}_m^{(l)}) \sigma_X^2 + \sigma_W^2$ is the variance of $\mathbf{y}_{\mathrm{E},l}$ with respect to the Gaussian-distributed input $\mathfrak{M}_{q_{l-1}}(\mathbf{x}_d^{(l-1)})$ transmitted from the m^{th} TA of Node $l-1$. Accordingly, the PDF of $\mathbf{y}_{\mathrm{E},l}$ is obtained by

$$p(\mathbf{y}_{\mathrm{E},l}) = \frac{1}{M_{l-1}} \sum_{m=1}^{M_{l-1}} p\left(\mathbf{y}_{\mathrm{E},l} | \mathbf{x}_a^{(l-1)}\right). \tag{23}$$

2) Finite-Alphabet Input: In this case, Eve's achievable data rate using MRC is expressed as

$$R_{\mathrm{E}}^{(L)} = \frac{1}{L} \sum_{l=1}^{L} \left(\frac{1}{M_{l-1}} R_{\mathrm{E}a}^{(l)} + \frac{1}{K_{l-1}} R_{\mathrm{E}d}^{(l)}\right), \tag{24}$$

where $R_{\mathrm{E}a}^{(l)}$ and $R_{\mathrm{E}d}^{(l)}$ denote the achievable data rates of the TA information $\mathbf{x}_a^{(l-1)}$ and the APSK information $\mathbf{x}_d^{(l-1)}$ gleaned by Eve, respectively, in the l^{th} hop, if Eve could successfully demap them. Concretely, $R_{\mathrm{E}a}^{(l)}$ and $R_{\mathrm{E}d}^{(l)}$ are calculated using (25) and (26), respectively, where the $N_{\mathrm{E}} \times 1$ vectors $\mathbf{q}_{m,m'}^{(l)} = \mathbf{g}_m s_k - \mathbf{g}_{m'} s_k$ and $\mathbf{q}_{m,m'}^{(l)k,k'} = \mathbf{g}_m s_k - \mathbf{g}_{m'} s_{k'}$, associated with $s_k^{(l)}, s_{k'}^{(l)} \in \mathfrak{M}_{q_{l-1}}(\cdot)$, $k, k' = 1, 2, \cdots, K_{l-1}$, $m, m' = 1, 2, \cdots, M_{l-1}$. Moreover, $\mathscr{E}_z\{\cdot\}$ stands for the expectation with respect to Eve's received AWGN, i.e., $\mathbf{z}_{\mathrm{E},l}$ in (2).

As shown in (25) and (26), for a given channel realization, we have $\lim_{\rho \to +\infty} R_{\mathrm{E}a}^{(l)}(\rho) = \log_2 M_{l-1}$ and $\lim_{\rho \to +\infty} R_{\mathrm{E}d}^{(l)}(\rho) = \log_2 K_{l-1}$. Consequently, as ρ tends to infinity, the limit of Eve's instantaneous data rate $R_{\mathrm{E}}^{(L)}$ using MRC becomes

$$\lim_{\rho \to +\infty} R_{\mathrm{E}}^{(L)}(\rho) = \frac{1}{L} \sum_{l=1}^{L} \left(\frac{\log_2 M_{l-1}}{M_{l-1}} + \frac{\log_2 K_{l-1}}{K_{l-1}}\right). \tag{27}$$

$$R_{\mathrm{D}}^{(l)} = \log_2(M_{l-1}K_{l-1}) - \frac{1}{M_{l-1}K_{l-1}} \sum_{m=1}^{M_{l-1}} \sum_{k=1}^{K_{l-1}} \mathscr{E}_z\Bigg\{ \log_2 \Bigg(1 + \underbrace{\sum_{\substack{m'=1 \\ (m',k')\neq(m,k)}}^{M_{l-1}} \sum_{k'=1}^{K_{l-1}} \exp\left(-\rho\left[\left(\mathbf{d}_{m,m'}^{(l)k,k'} + \mathbf{z}_{\mathrm{D},l}\right)^{\dagger}\left(\mathbf{d}_{m,m'}^{(l)k,k'} + \mathbf{z}_{\mathrm{D},l}\right) - \mathbf{z}_{\mathrm{D},l}^{\dagger}\mathbf{z}_{\mathrm{D},l}\right]\right)\Bigg)\Bigg\}}_{f(\rho)} \tag{16}$$

$$R_{\mathrm{E}a}^{(l)} = \log_2 M_{l-1} - \frac{1}{M_{l-1}K_{l-1}} \sum_{m=1}^{M_{l-1}} \sum_{k=1}^{K_{l-1}} \mathscr{E}_z\Bigg\{ \log_2 \Bigg(\sum_{m'=1}^{M_{l-1}} \exp\left(-\rho\left[\left(\mathbf{q}_{m,m'}^{(l)} + \mathbf{z}_{\mathrm{E},l}\right)^{\dagger}\left(\mathbf{q}_{m,m'}^{(l)} + \mathbf{z}_{\mathrm{E},l}\right) - \mathbf{z}_{\mathrm{E},l}^{\dagger}\mathbf{z}_{\mathrm{E},l}\right]\right)\Bigg)\Bigg\} \tag{25}$$

$$\begin{aligned} R_{\mathrm{E}d}^{(l)} = \log_2 K_{l-1} - \frac{1}{M_{l-1}K_{l-1}} \sum_{m=1}^{M_{l-1}} \sum_{k=1}^{K_{l-1}} \mathscr{E}_z\Bigg\{ & \log_2 \Bigg(\sum_{m'=1}^{M_{l-1}} \sum_{k'=1}^{K_{l-1}} \exp\left(-\rho\left(\mathbf{q}_{m,m'}^{(l)k,k'} + \mathbf{z}_{\mathrm{E},l}\right)^{\dagger}\left(\mathbf{q}_{m,m'}^{(l)k,k'} + \mathbf{z}_{\mathrm{E},l}\right)\right)\Bigg) \\ & - \log_2 \Bigg(\sum_{m'=1}^{M_{l-1}} \exp\left(-\rho\left(\mathbf{q}_{m,m'}^{(l)} + \mathbf{z}_{\mathrm{E},l}\right)^{\dagger}\left(\mathbf{q}_{m,m'}^{(l)} + \mathbf{z}_{\mathrm{E},l}\right)\right)\Bigg)\Bigg\} \end{aligned} \tag{26}$$

B. Maximum-Gain Selection (MGS)

In this scenario, Eve's instantaneous data rate is expressed using

$$C_{\mathrm{E,MGS}} = \min\left(C_{\mathrm{D}}^{(1)}, C_{\mathrm{D}}^{(2)}, \cdots, C_{\mathrm{D}}^{(l^*-1)}, C_{\mathrm{E}}^{(l^*)}\right) \tag{28}$$

for Gaussian-distributed inputs, and

$$R_{\mathrm{E,MGS}} = \min\left(R_{\mathrm{D}}^{(1)}, R_{\mathrm{D}}^{(2)}, \cdots, R_{\mathrm{D}}^{(l^*-1)}, R_{\mathrm{E}}^{(l^*)}\right) \tag{29}$$

for finite-alphabet inputs, where $C_{\mathrm{E}}^{(l^*)}$ and $R_{\mathrm{E}}^{(l^*)}$ denote Eve's achievable data rates gleaned from the SM signals conveyed by Node l^*-1, using MGS, in the cases of Gaussian-distributed and finite-alphabet inputs, respectively. Moreover, $C_{\mathrm{D}}^{(l)}$ and $R_{\mathrm{D}}^{(l)}$ are given by (10) and (16), respectively, for $l = 1, 2, \cdots, l^*-1$.

1) Gaussian-Distributed Input: In this case, the probability that Eve can successfully demap the Gaussian information transmitted by any node over the legitimate link is 0. Therefore, Eve's achievable data rate upon using MGS in the $(l^*)^{\mathrm{th}}$ hop is given by

$$C_{\mathrm{E}}^{(l^*)} = \frac{1}{M_{l^*-1}} C_{\mathrm{E}a}^{(l^*)}, \tag{30}$$

where $C_{\mathrm{E}a}^{(l^*)}$ is the data rate of $\mathbf{x}_a^{(l^*-1)}$ potentially available for Eve, provided that she could successfully demap it. In detail, $C_{\mathrm{E}a}^{(l^*)}$ is calculated using

$$\begin{aligned} C_{\mathrm{E}a}^{(l^*)} = \frac{1}{M_{l^*-1}} \sum_{m=1}^{M_{l^*-1}} \int_{\bar{y}_{\mathrm{E},l^*}} & p\left(\bar{y}_{\mathrm{E},l^*} | \mathbf{x}_a^{(l^*-1)}\right) \\ & \times \log_2 \frac{p\left(\bar{y}_{\mathrm{E},l^*} | \mathbf{x}_a^{(l^*-1)}\right)}{p(\bar{y}_{\mathrm{E},l^*})} d\bar{y}_{\mathrm{E},l^*}, \end{aligned} \tag{31}$$

where $\bar{y}_{\mathrm{E},l^*} = (\mathbf{g}_m^{(l^*)})^{\dagger}\mathbf{y}_{\mathrm{E},l^*}$ is the equivalent signal used by Eve's detector in the $(l^*)^{\mathrm{th}}$ hop, as shown in (7) and (8). Since the input $\mathfrak{M}_{q_{l^*-1}}(\mathbf{x}_d^{(l^*-1)})$ is complex Gaussian distributed, the conditional PDF of $\bar{y}_{\mathrm{E},l^*}$ given the TA information $\mathbf{x}_a^{(l^*-1)}$ is obtained by

$$p\left(\bar{y}_{\mathrm{E},l^*} | \mathbf{x}_a^{(l^*-1)}\right) = \frac{1}{\pi\sigma_{\bar{y}_{\mathrm{E},l^*}}^2} \exp\left(-\frac{|\bar{y}_{\mathrm{E},l^*}|^2}{\sigma_{\bar{y}_{\mathrm{E},l^*}}^2}\right), \tag{32}$$

where $\sigma_{\bar{y}_{\mathrm{E},l^*}}^2 = [(\mathbf{g}_m^{(l^*)})^{\dagger}(\mathbf{g}_m^{(l^*)})]^2\sigma_X^2 + (\mathbf{g}_m^{(l^*)})^{\dagger}(\mathbf{g}_m^{(l^*)})\sigma_W^2$ is the variance of $\bar{y}_{\mathrm{E},l^*}$ with respect to the Gaussian-distributed input $\mathfrak{M}_{q_{l^*-1}}(\mathbf{x}_d^{(l^*-1)})$ transmitted from the m^{th} TA of Node l^*-1. Thus, the PDF of $\bar{y}_{\mathrm{E},l^*}$ is

$$p(\bar{y}_{\mathrm{E},l^*}) = \frac{1}{M_{l-1}} \sum_{m=1}^{M_{l^*-1}} p\left(\bar{y}_{\mathrm{E},l^*} | \mathbf{x}_a^{(l^*-1)}\right). \tag{33}$$

2) Finite-Alphabet Input: Since Eve is unable to flawlessly demap the SM signals in any hop, her instantaneous data rate upon using MGS of the $(l^*)^{\mathrm{th}}$ hop is given by

$$R_{\mathrm{E}}^{(l^*)} = \frac{1}{M_{l^*-1}} R_{\mathrm{E}a}^{(l^*)} + \frac{1}{K_{l^*-1}} R_{\mathrm{E}d}^{(l^*)}, \tag{34}$$

where $R_{\mathrm{E}a}^{(l^*)}$ and $R_{\mathrm{E}d}^{(l^*)}$ denote the achievable data rates pertaining to the TA information $\mathbf{x}_a^{(l^*-1)}$ and the APSK information $\mathbf{x}_d^{(l^*-1)}$ potentially available for Eve, respectively, in the $(l^*)^{\mathrm{th}}$ hop, provided that Eve could successfully demap them. Upon replacing l by l^* in (25) and (26), $R_{\mathrm{E}a}^{(l^*)}$ and $R_{\mathrm{E}d}^{(l^*)}$ will be obtained.

For a given channel realization, we have $\lim_{\rho\to+\infty} R_{\mathrm{E}a}^{(l^*)}(\rho) = \log_2 M_{l^*-1}$ and $\lim_{\rho\to+\infty} R_{\mathrm{E}d}^{(l^*)}(\rho) = \log_2 K_{l^*-1}$. Consequently, as ρ tends to infinity, the limit of Eve's instantaneous data rate $R_{\mathrm{E}}^{(l^*)}$ using MGS is given by

$$\lim_{\rho\to+\infty} R_{\mathrm{E}}^{(l^*)}(\rho) = \frac{\log_2 M_{l^*-1}}{M_{l^*-1}} + \frac{\log_2 K_{l^*-1}}{K_{l^*-1}}. \tag{35}$$

VI. Secrecy Rate of the Secret Key in Multi-Hop Wiretap Ad-Hoc Networks

The secrecy rate of a wiretap channel is defined as the positive difference between the achievable data rates obtained by the legitimate link and the wiretapper link, i.e., given that the legitimate link is of better state than the wiretapper link. For multi-hop wiretap *ad-hoc* networks relying on the proposed secret key generation, the instantaneous secrecy rate with the Gaussian-distributed input is expressed as

$$C_{s,\mathrm{MRC}} = \max(0, C_\mathrm{D} - C_{\mathrm{E},\mathrm{MRC}}) \tag{36}$$

if MRC is utilised by Eve, and

$$C_{s,\mathrm{MGS}} = \max(0, C_\mathrm{D} - C_{\mathrm{E},\mathrm{MGS}}) \tag{37}$$

if Eve adopts MGS. With the finite-alphabet input, the instantaneous secrecy rate is denoted by

$$R_{s,\mathrm{MRC}} = \max(0, R_\mathrm{D} - R_{\mathrm{E},\mathrm{MRC}}) \tag{38}$$

when Eve employs MRC, and

$$R_{s,\mathrm{MGS}} = \max(0, R_\mathrm{D} - R_{\mathrm{E},\mathrm{MGS}}) \tag{39}$$

when Eve utilises MGS. Herein, C_D, R_D, $C_{\mathrm{E},\mathrm{MRC}}$, $R_{\mathrm{E},\mathrm{MRC}}$, $C_{\mathrm{E},\mathrm{MGS}}$, and $R_{\mathrm{E},\mathrm{MGS}}$ are given by (9), (15), (18), (19), (28), and (29), respectively.

To evaluate the security performance of our physical-layer secret key exploited in multi-hop *ad-hoc* networks, we numerically evaluate the ergodic secrecy rate and the secrecy outage probability based on the expressions in Sections IV and V, for i.i.d. Rayleigh fading channels $h_{nm}^{(l)}$ and $g_{nm}^{(l)}$, $l = 1, 2, \cdots, L$, $m = 1, 2, \cdots, M_{l-1}$, $n = 1, 2, \cdots, M_l, N_\mathrm{E}$.

A. Ergodic Secrecy Rate

The ergodic secrecy rates under study are defined as $\mathscr{E}\{C_{s,\mathrm{MRC}}\}$, $\mathscr{E}\{C_{s,\mathrm{MGS}}\}$, $\mathscr{E}\{R_{s,\mathrm{MRC}}\}$, $\mathscr{E}\{R_{s,\mathrm{MGS}}\}$, where $C_{s,\mathrm{MRC}}$, $C_{s,\mathrm{MGS}}$, $R_{s,\mathrm{MRC}}$, $R_{s,\mathrm{MGS}}$ are given by (36), (37), (38), (39), respectively.

In Fig. 7, the ergodic secrecy rates $\mathscr{E}\{C_{s,\mathrm{MRC}}\}$ and $\mathscr{E}\{C_{s,\mathrm{MGS}}\}$ are compared for Gaussian-distributed inputs within $L = 2, 4, 8$-hop wiretap networks, where two scenarios are investigated: $M_l = N_\mathrm{E} = 2$, i.e., each node has 2 antennas, and $M_l = N_\mathrm{E} = 4$, $l = 0, 1, \cdots, L$. For the sake of comparison, the data rates $\mathscr{E}\{C_\mathrm{D}\}$ achieved over the legitimate link with Gaussian-distributed inputs are also plotted in this figure, where C_D is given by (9). The gaps between $\mathscr{E}\{C_\mathrm{D}\}$ and $\mathscr{E}\{C_{s,\mathrm{MRC}}\}$, $\mathscr{E}\{C_{s,\mathrm{MGS}}\}$ are equivalent to $\mathscr{E}\{C_{\mathrm{E},\mathrm{MRC}}\}$ and $\mathscr{E}\{C_{\mathrm{E},\mathrm{MGS}}\}$, i.e., Eve's achievable data rates with Gaussian-distributed inputs. As shown in this figure, the gaps between achievable data rates over the legitimate link and the corresponding secrecy rates are negligible. Explicitly, this implies that Eve's attempts to detect the confidential information forwarded over the legitimate link, using either MRC or MGS, are nullified by our physical-layer secret key using Gaussian-distributed inputs, within multi-hop wiretap *ad-hoc* networks.

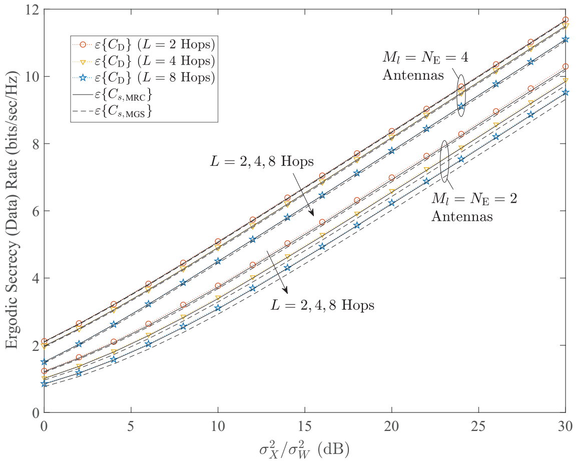


Fig. 7. Ergodic secrecy rates offered by our physical-layer secret key with Gaussian-distributed inputs, $\mathscr{E}\{C_{s,\mathrm{MRC}}\}$ and $\mathscr{E}\{C_{s,\mathrm{MGS}}\}$, in $L = 2, 4, 8$-hop wiretap networks for the scenarios: (i) $M_l = N_\mathrm{E} = 2$, and (ii) $M_l = N_\mathrm{E} = 4$. Also shown is the achievable data rate of the legitimate link, $\mathscr{E}\{C_\mathrm{D}\}$, in these scenarios.

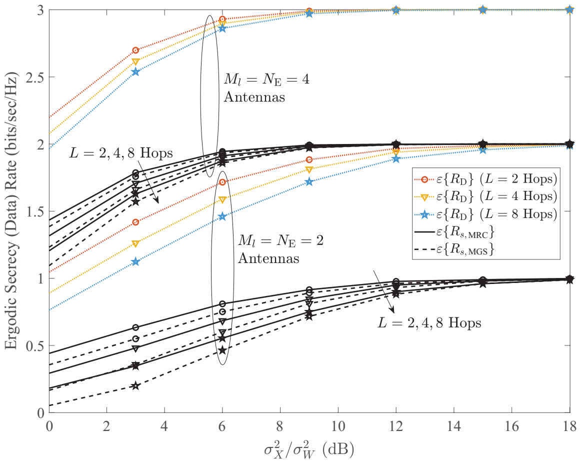


Fig. 8. Ergodic secrecy rates offered by our physical-layer secret key with BPSK input, $\mathscr{E}\{R_{s,\mathrm{MRC}}\}$ and $\mathscr{E}\{R_{s,\mathrm{MGS}}\}$, in $L = 2, 4, 8$-hop wiretap networks for the scenarios: (i) $M_l = N_\mathrm{E} = 2$, and (ii) $M_l = N_\mathrm{E} = 4$. Also shown is the achievable data rate of the legitimate link, $\mathscr{E}\{R_\mathrm{D}\}$, in these scenarios.

In Figs. 8 and 9, the ergodic secrecy rates $\mathscr{E}\{R_{s,\mathrm{MRC}}\}$ and $\mathscr{E}\{R_{s,\mathrm{MGS}}\}$ are compared for BPSK and QPSK sources, respectively, within our $L = 2, 4, 8$-hop wiretap networks, where the scenarios of $M_l = N_\mathrm{E} = 2$ and $M_l = N_\mathrm{E} = 4$ are investigated, $l = 0, 1, \cdots, L$. The data rates $\mathscr{E}\{R_\mathrm{D}\}$ attained over the legitimate link using BPSK and QPSK are plotted as well, where R_D is given by (15). We note that the gaps between $\mathscr{E}\{R_\mathrm{D}\}$ and $\mathscr{E}\{R_{s,\mathrm{MRC}}\}$, $\mathscr{E}\{R_{s,\mathrm{MGS}}\}$ are equivalent to $\mathscr{E}\{R_{\mathrm{E},\mathrm{MRC}}\}$ and $\mathscr{E}\{R_{\mathrm{E},\mathrm{MGS}}\}$. Explicitly, Eve's achievable data rate with the finite-alphabet input converges to a constant of $\log_2 M_l/M_l + \log_2 K_l/K_l$, as shown in Figs. 8 and 9.

Figs. 7-9 reveal that both the secrecy rates and the achievable data rates of the legitimate link are reduced upon increasing the number of hops. On the other hand, as the number of transmit/receive antennas or APSK constellation points increases, the gaps between data rates attained over the legitimate link and their corresponding secrecy rates will

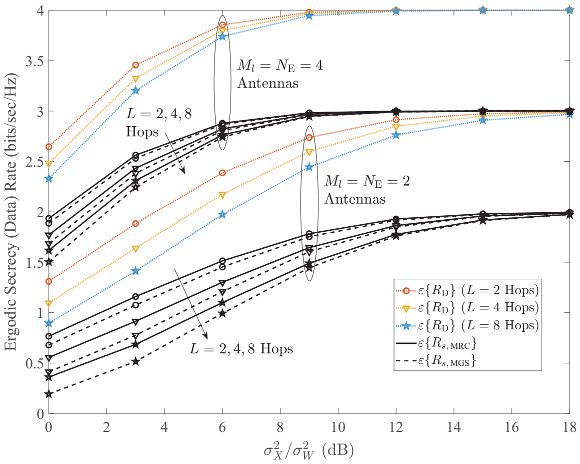


Fig. 9. Ergodic secrecy rates offered by our physical-layer secret key with QPSK input, $\mathscr{E}\{R_{s,\text{MRC}}\}$ and $\mathscr{E}\{R_{s,\text{MGS}}\}$, in $L = 2, 4, 8$-hop wiretap networks for the scenarios: (i) $M_l = N_\text{E} = 2$, and (ii) $M_l = N_\text{E} = 4$. Also shown is the achievable data rate of the legitimate link, $\mathscr{E}\{R_\text{D}\}$, in these scenarios.

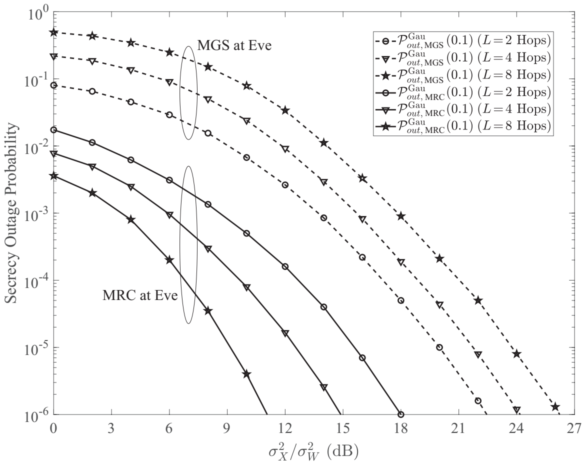


Fig. 10. Secrecy outage probabilities of our physical-layer secret key with Gaussian-distributed inputs and $M_l = N_\text{E} = 2$, $\mathcal{P}^{\text{Gau}}_{out,\text{MRC}}(0.1)$ and $\mathcal{P}^{\text{Gau}}_{out,\text{MGS}}(0.1)$, in $L = 2, 4, 8$-hop wiretap networks.

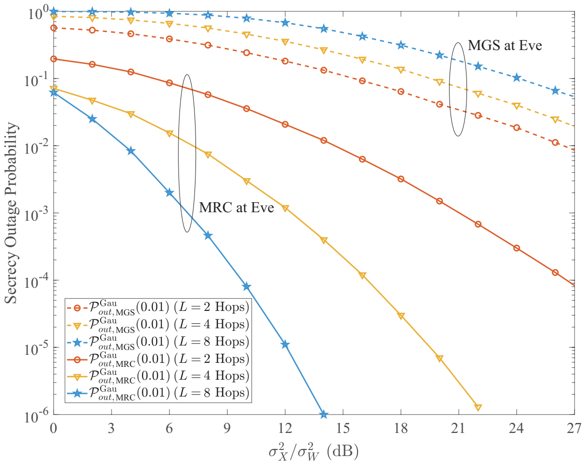


Fig. 11. Secrecy outage probabilities of our physical-layer secret key with Gaussian-distributed inputs and $M_l = N_\text{E} = 4$, $\mathcal{P}^{\text{Gau}}_{out,\text{MRC}}(0.01)$ and $\mathcal{P}^{\text{Gau}}_{out,\text{MGS}}(0.01)$, in $L = 2, 4, 8$-hop wiretap networks.

be reduced. Moreover, the multi-hop wiretap *ad-hoc* networks under study achieve better security performance when Eve utilises MRC, instead of MGS. The main reason behind this is that Eve's achievable data rate will be determined by the minimum one of all legitimate hops when using MRC, while it will be determined by the minimum one of the first $l^* - 1$ legitimate hops when using MGS, as reflected by the comparison between (18), (19) and (28), (29).

B. Secrecy Outage Probability

The secrecy outage probability is defined as the probability that the instantaneous secrecy rate is below a target data rate [38]. For multi-hop wiretap *ad-hoc* networks relying on our physical-layer secret key, the secrecy outage probabilities are expressed as

$$\mathcal{P}^{\text{Gau}}_{out,\text{MRC}}(\epsilon) = \Pr\{C_{s,\text{MRC}} < (1-\epsilon)C_\text{D}\} \tag{40}$$

if Eve utilises MRC for detecting Gaussian-distributed inputs,

$$\mathcal{P}^{\text{Gau}}_{out,\text{MGS}}(\epsilon) = \Pr\{C_{s,\text{MGS}} < (1-\epsilon)C_\text{D}\} \tag{41}$$

if Eve uses MGS for detecting Gaussian-distributed inputs,

$$\mathcal{P}^{\text{Fin}}_{out,\text{MRC}}(\epsilon) = \Pr\{R_{s,\text{MRC}} < (1-\epsilon)R_\text{D}\} \tag{42}$$

if Eve employs MRC in the presence of finite-alphabet inputs, and

$$\mathcal{P}^{\text{Fin}}_{out,\text{MGS}}(\epsilon) = \Pr\{R_{s,\text{MGS}} < (1-\epsilon)R_\text{D}\} \tag{43}$$

if Eve utilises MGS for extracting the legitimate finite-alphabet inputs. Herein, $\epsilon < 1$ is a predetermined small positive quantity and the target secrecy rates are $(1-\epsilon)C_\text{D}$ and $(1-\epsilon)R_\text{D}$, which are almost identical to the achievable data rates of the legitimate link. In particular, $\epsilon \to 0$ implies a near-zero rate for Eve.

In Figs. 10 and 11, secrecy outage probabilities of multi-hop wiretap *ad-hoc* networks using the physical-layer secret key with Gaussian-distributed inputs are plotted versus the SNR σ_X^2/σ_W^2 for the setting of $M_l = N_\text{E} = 2$ and $M_l = N_\text{E} = 4$, respectively. Upon using more antennas, the security performance becomes better, and therefore the parameter ϵ may be set to a smaller number. For example, $\epsilon = 0.1$ when $M_l = N_\text{E} = 2$ and $\epsilon = 0.01$ when $M_l = N_\text{E} = 4$. As shown in these figures, the secrecy outage probability of the multi-hop wiretap networks under study in the case of MRC used by Eve is lower than that in the case of MGS. Additionally, as the number of hops increases, the secrecy outage probability is reduced if Eve adopts MRC, while it is increased if Eve uses MGS. The main reason behind this phenomenon is that the achievable data rate of the Gaussian-distributed input detected by Eve approaches 0. Upon increasing the number of hops, the secrecy rate of MRC adopted by Eve becomes more stable than that of MGS used at Eve.

Furthermore, the secrecy outage probabilities of multi-hop wiretap *ad-hoc* networks using our physical-layer secret key

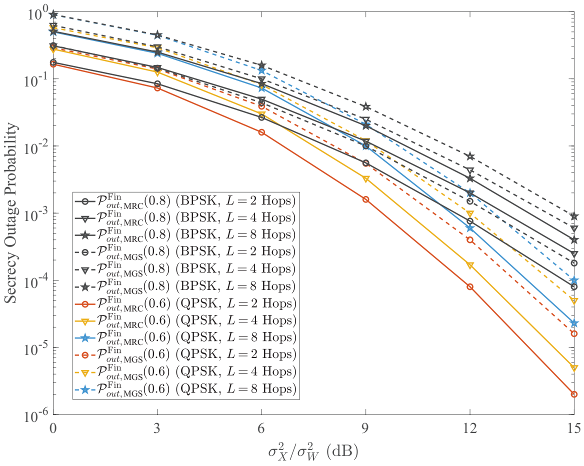


Fig. 12. Secrecy outage probabilities of our physical-layer secret key with BPSK and QPSK inputs, $\mathcal{P}^{\mathrm{Fin}}_{out,\mathrm{MRC}}(\epsilon)$ and $\mathcal{P}^{\mathrm{Fin}}_{out,\mathrm{MGS}}(\epsilon)$, in $L = 2, 4, 8$-hop wiretap networks with $M_l = N_{\mathrm{E}} = 2$.

with BPSK and QPSK inputs are reported in Fig. 12, where the number of antennas at each node is $M_l = N_{\mathrm{E}} = 2$. As shown in this figure, the secrecy outage probability decreases upon increasing the number of APSK constellation points, even if ϵ gets smaller. Moreover, as the number of hops increases, the secrecy outage probability of finite-alphabet inputs decreases for both MRC and MGS used by Eve.

VII. Conclusion

In this paper, a physical-layer secret key generation via CQI-mapped SM was developed for the multi-hop MIMO wiretap channels of *ad-hoc* and IoT networks. The security performance in this context was formulated based on the analysis of achievable data rates over the legitimate link and in the wiretapper link, for both Gaussian-distributed and finite-alphabet inputs. Specifically, concerning the vulnerabilities that result from multiple hops of the intended SM messages in the *ad-hoc* networks, we investigated the scenarios where Eve distributed multi-antenna frontends to monitor all legitimate nodes' transmitting and exploited receive diversity techniques, namely MRC and MGS, in their detection of multiple SM signal copies received from the legitimate link. In other words, Eve's maximised wiretapping capability was investigated in this work. Our theoretical analysis and numerical results of ergodic secrecy rate and secrecy outage probability substantiated the benefits of our physical-layer secret key in terms of improving the PLS for multi-hop MIMO wiretap *ad-hoc* networks. Moreover, this information source controlled PLS solution achieved better security, when MRC is adopted by Eve, rather than MGS. Furthermore, this solution could lead to a plainer transmission medium and provide more freedom for the *ad-hoc* and IoT network design.

Acknowledgment

The authors would like to thank the editor and the anonymous reviewers for their valuable comments to improve the presentation of this paper.

References

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016.

[2] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, Feb. 2017.

[3] J. Hamamreh, H. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Sept. 2019.

[4] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[5] H. Moosavi and F. M. Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 1928–1939, Sept. 2016.

[6] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for iot: Challenges and opportunities," *IEEE Internet Things J.*, Oct. 2019.

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. Journ.*, vol. 28, pp. 656–715, 1949.

[8] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journ.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[9] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.

[10] C. Jeong, I. Kim, , and D. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[11] H. Wang, M. Luo, Q. Yin, and X. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[12] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[13] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 621–634, Mar. 2019.

[14] Z. Kong, S. Yang, D. Wang, and L. Hanzo, "Robust beamforming and jamming for enhancing the physical layer security of full duplex radios," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3151–3159, Dec. 2019.

[15] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Jamming based on an ephemeral key to obtain everlasting security in wireless environments," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6072–6081, Nov. 2015.

[16] Y. Yang and B. Jiao, "Artificial-noise strategy for single-antenna systems over multi-path fading channels," in *Proc. IEEE Int. Wireless Commun. and Mobile Computing Conf. (IWCMC'15)*, Aug. 2015.

[17] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, June 2017.

[18] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6190–6204, Sept. 2018.

[19] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[20] R. Nakai and S. Sugiura, "Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 431–444, Feb. 2019.

[21] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 650–660, Sept. 2011.

[22] M. Edman, A. Kiayias, Q. Tang, and B. Yener, "On the security of key extraction from measuring physical quantities," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1796–1806, Aug. 2016.

[23] Y. Yang and B. Jiao, "Information-guided channel-hopping for high data rate wireless communication," *IEEE Commun. Lett.*, vol. 12, no. 4, pp. 225–227, Apr. 2008.

[24] M. D. Renzo, H. Haas, A. Ghrayeb, S. Sugiura, and L. Hanzo, "Spatial modulation for generalized MIMO: Challenges, opportunities, and implementation," *Proc. IEEE*, vol. 102, no. 1, pp. 56–103, Jan. 2014.

[25] C. Liu, M. Ma, Y. Yang, and B. Jiao, "Optimal spatial-domain design for spatial modulation capacity maximization," *IEEE Commun. Lett.*, vol. 10, no. 6, pp. 1092–1095, June 2016.

[26] Y. Shi, M. Ma, Y. Yang, and B. Jiao, "Optimal power allocation in spatial modulation systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1646–1655, Mar. 2017.

[27] F. Wu, R. Zhang, L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, Jan. 2016.

[28] Z. Huang, Z. Gao, and L. Sun, "Anti-eavesdropping scheme based on quadrature spatial modulation," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 532–535, Mar. 2017.

[29] C. Liu, L. Yang, and W. Wang, "Secure spatial modulation with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 838–841, Dec. 2017.

[30] Z. Bouida, A. Stavridis, A. Ghrayeb, H. Haas, and M. Hasna, "Precoded spatial modulation for the wiretap channel with relay selection and cooperative jamming," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC'17)*, Mar. 2017.

[31] S. Guo, H. Zhang, P. Zhang, and D. Yuan, "Link-adaptive mapper designs for space-shift-keying-modulated MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8087–8100, Oct. 2016.

[32] S. Guo, H. Zhang, P. Zhang, and D. Yuan, "Adaptive mapper design for spatial modulation with lightweight feedback overhead," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 8940–8950, Oct. 2017.

[33] Z. Sun, Y. Xiao, P. Yang, S. Li, and W. Xiang, "Transmit antenna selection schemes for spatial modulation systems: Search complexity reduction and large-scale MIMO applications," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8010–8021, Sept. 2017.

[34] F. Shu, Z. Wang, R. Chen, Y. Wu, and J. Wang, "Two high-performance schemes of transmit antenna selection for secure spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8969–8973, Sept. 2018.

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

[36] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[37] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.

[38] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Sym. Inf. Theory (ISIT'06)*, July 2006.