Secrecy Outage Analysis for Alamouti Space-Time Block Coded Non-orthogonal Multiple Access

Meiling Li, Hu Yuan, Xinwei Yue, Sami Muhaidat, Carsten Maple and Mehrdad Dianati

***Abstract*—This letter proposed a novel transmission technique for physical layer security by applying the Alamouti Space-Time Block Coded Non-orthogonal Multiple Access (STBC-NOMA) scheme. The secure outage performance under both perfect successive interference cancellation (pSIC) and imperfect successive interference cancellation (ipSIC) are investigated. In particular, novel exact and asymptotic expressions of secrecy outage probability are derived. Numerical and theoretical results are presented to corroborate the derived expressions and to demonstrate the superiority of STBC-NOMA and its ability to enhance the secrecy outage performance compared to conventional NOMA.**

***Index Terms*—Alamouti space-time block coding, Non-orthogonal Multiple Access, Secure outage probability.**

I. Introduction

NON-orthogonal multiple access (NOMA) has been envisaged as a promising technique for the next generation wireless communication systems to realize massive connectivity and higher system spectral efficiency [1]. However, due to the broadcast nature of of radio propagation, NOMA can be vulnerable to eavesdropping, which poses a challenge for realizing secure wireless transmissions, which poses a challenge to realize secure wireless transmission.

The concept of physical layer security (PLS) has attracted the attention of the research community to secure the transmission in NOMA systems. The authors of [2] investigated the secrecy outage behavior of single antenna and multiple antenna transmission scenarios for NOMA networks. The authors in [3] investigated the performance of a secure NOMA-enabled mobile edge computing network, where the optimal secrecy offloading rate and power allocation were analyzed and presented in closed-form expressions. However, the perfect successive interference cancellation (pSIC) scheme is conducted at legitimate users (LUs) and eavesdroppers (Eves) in the aforementioned articles. This assumption overestimates users detection capability and resulted in the performance deviation. Relaxing this assumption, the authors in [4] investigated the impact of physical layer secrecy on the performance of a NOMA system, where the imperfect successive interference cancellation (ipSIC) was considered. The authors in [5] studied the secrecy outage behaviours of multiple-input-multiple-output (MIMO) NOMA, assuming max-min transmit antenna selection. In [6], the authors optimised transmission power by taking into account both the bounded CSI error and Gaussion CSI error models. The authors further considered an artificial noise scheme to improve the secure performance of the considered network [7].

To exploit the spectral efficiency, a downlink coordinated two-point NOMA system has been discussed in [8] by utilizing Alamouti space-time block coding (STBC). In [9], the authors proposed a two-phase NOMA cooperative relaying scheme in which Alamouti STBC was employed. Closed-form expressions for outage probability and ergodic sum capacity were derived over Rayleigh fading channels. In [10], [11], the authors combined NOMA with Alamouti STBC to improve system diversity order of NOMA systems.

To the best knowledge of the authors, the secrecy performance of STBC-NOMA has not been investigated in the literature. Moreover, the majority work of NOMA assumed pSIC, which is not sensible in practice. Motivated by this, we investigate the secrecy outage performance of STBC-NOMA over Rayleigh fading channels. Specifically, we derive exact and asymptotic expressions for secrecy outage probability (SOP) of all legitimate users with both pSIC and ipSIC. It can be deduced that the secrecy outage performance can be obviously improved by STBC-NOMA and the diversity order of $2l$ is achieved under pSIC case. However, a zero diversity order is under ipSIC case due to the imperfect interference cancelling which results the error floor.

The remainder of this letter is organized as follows. The system model is presented in Section II. The security outage performance is analysed in Section III. Section IV presents the simulation and numerical results. Finally, conclusions is given in Section V with further discussions.

II. System Model

Consider a downlink NOMA system consisting of L LUs and one Eve with single antenna. The base station (BS)

This work was supported in part by Key Research and Development Program of Shanxi (Grant 201903D121117), Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi (Grant 201802090), in part by CiCi3DP and in part by KITSX1331; in part by Alan Turing Institute under EPSRC grant (EP/N510129/1) and PETRAS, the National Centre of Excellence for IoT Systems Cybersecurity grant (EP/S035362/1); in part by Natural Science Foundation of Beijing Municipality (4204099), Science and Technology Project of Beijing Municipal Education Commission (KM202011232003). *(Corresponding author: Hu Yuan.)*

M. Li is with School of Electronics Information Engineering, Taiyuan University of Science and Technology, 030024 Taiyuan, China (e-mail: meiling_li@126.com).

H. Yuan, C. Maple and M. Dianati are with the WMG, University of Warwick, Coventry, CV4 7AL, UK (e-mail: H.Yuan.4@warwick.ac.uk, CM@warwick.ac.uk, m.dianati@warwick.ac.uk).

X. Yue is with School of Information Communication and Engineering, Beijing Information Science Technology University, 100192, China (e-mail: xinwei.yue@bistu.edu.cn).

S. Muhaidat is with Center for Cyber-Physical Systems, Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, 127788, The United Arab Emirates (e-mail: muhaidat@ieee.org).

transmit superimposed symbols over two transmit antenna using the Alamouti code [11]. NOMA requires the knowledge of all LUs, and the condition that LUs have different channels conditions [2]. Let P, k_l, and a_l denote the transmit power of the BS, information symbol, and power allocation factor of the l-th sorted LU, respectively. The power allocation factors are defined as $a_1 > a_2 > ... > a_L$ and $\sum_{i=1}^{L} \sqrt{a_i} = 1$. The received signals at user l from the BS is $r_l = \|\mathbf{h}_l\|_F^2 \sum_{L}^{i=1} k_i \sqrt{a_i P/2} + n_l$, $\mathbf{h}_l = [h_{S_1 U_l}, h_{S_2 U_l}]^{\mathsf{T}}$ are the Rayleigh channel gains from the BS to l-th LU, which is a vector from two antennas to achieve transmitting diversity, where $h_{S_i U_l} \sim CN\left(0, \lambda_0\right), i \in \{1, 2\}$ and sorted in ascending order as $\|\mathbf{h}_1\|_F^2 \leq \|\mathbf{h}_{_2}\|_F^2 \leq \cdots \leq \|\mathbf{h}_{_L}\|_F^2$ [4]. The notation $||.||_F^2$ denotes the Frobenius norm of a vector and $n_l \sim CN\left(0, 1\right)$ is the equivalent normalized additive Gaussion noise. The assumption is that the channel gains of LUs and Eve are independent identical distributed. Note that $\mathbf{h}_I = [h_I^{S_1 U_l}, h_I^{S_2 U_l}]^{\mathsf{T}}$ denotes the residual interference where $h_I^{S_i U_l} \sim CN\left(0, \lambda_I\right), i \in \{1, 2\}$.

Following the principle of NOMA, we consider the l-th ($l > 1$) LU utilises ipSIC to decode its own signal by treating stronger users as interference. Here, we assume ipSIC case that the interference introduced by the ipSIC implementation being considered into the analysis. Let $w = 0$ and $w \neq 0$ represent the pSIC and ipSIC operations in the following sections, respectively. The instantaneous signal-to-interference plus noise ratio (SINR) of the l-th LU ($l < L$) can be expressed as[1]:

$$\gamma_l = \frac{\rho a_l ||\mathbf{h}_l||_F^2}{\sum_{k=l+1}^{L} a_k \rho ||\mathbf{h}_l||_F^2 + w\rho ||\mathbf{h}_I||_F^2 + 1}, \tag{1}$$

where $\rho = P/2$.

The SINR of the first user (LU$_1$) and L-th user (LU$_L$) can be written as :

$$\gamma_1 = \frac{\rho a_1 ||\mathbf{h}_1||_F^2}{\sum_{k=2}^{L} a_k \rho ||\mathbf{h}_1||_F^2 + 1}, \ \gamma_L = \frac{\rho a_L ||\mathbf{h}_L||_F^2}{\omega \rho ||\mathbf{h}_I||_F^2 + 1}. \tag{2}$$

Similarly, Eve will receive the same signal as the LUs via eavesdropping link. The equivalent received signal at the Eve is $r_E = \|\mathbf{h}_E\|_F^2 \sum_{L}^{i=1} k_i \sqrt{a_i P/2} + n_E$, where the entries of $\mathbf{h}_E = [h_{S_1 E}, h_{S_2 E}]^{\mathsf{T}}$ represent the channel gains from the BS to Eve with $h_{S_i E} \sim CN\left(0, \lambda_e\right), i \in \{1, 2\}$, and $n_E \sim CN\left(0, \Omega_e\right)$ is the channel noise in the eavesdropping link. When achieved SINR at Eve is below a threshold, Eve is not able to recover the source signal so the transmission can be regarded as relatively secure. Then, with the ipSIC assumption the SINR at Eve to detect the symbol of LU$_l$ can be expressed as:

$$\gamma_{E_l} = \frac{\rho_e a_l ||\mathbf{h}_e||_F^2}{\sum\limits_{k=l+1}^{L} a_k \rho_e ||\mathbf{h}_e||_F^2 + w\rho_e ||\mathbf{h}_{Ie}||_F^2 + 1}, \tag{3}$$

where $1 < l < L$, $\rho_e = P/2\Omega_e$, The entries of $\mathbf{h}_{Ie} = [h_I^{S_1 E}, h_I^{S_2 E}]^{\mathsf{T}}$ are the channel gains from the BS to Eve with $h_I^{S_i E} \sim CN\left(0, \lambda_{I_e}\right), i \in \{1, 2\}$. When $l = 1$ and $l = L$, the SINRs are:

$$\gamma_{E_1} = \frac{\rho_e a_1 ||\mathbf{h}_e||_F^2}{\sum_{k=2}^{L} a_k \rho_e ||\mathbf{h}_e||_F^2 + 1}, \gamma_{E_L} = \frac{\rho_e a_L ||\mathbf{h}_e|||_F^2}{w\rho_e ||\mathbf{h}_{Ie}||_F^2 + 1}. \tag{4}$$

It is noted that, we assume that the messages of $l - 1$ user have already been decoded before the eavesdropper tries to decode the message of $l - th$ user. Similar assumptions can be found in [4]. Obviously, the assumption overestimates the capability of eavesdropper and is pessimistic, then the results presented in this letter will be a lower bound of practical cases.

III. Performance Analysis

In this section, we focus on the SOP as a secrecy performance metric [4]. The event of secrecy outage is defined as that the secrecy capacity of the l-th user is less than the target secrecy rate R_l, $\log_2(1+\gamma_l) - \log_2(1+\gamma_{E_l}) < R_l$. When the channel capacity of user l is larger than the channel capacity of the Eve over R_l, the transmission from BS to user l can be considered secure [12], [13]. The exact and asymptotic expressions of SOP for both pSIC ($\omega = 0$) and ipSIC ($\omega \neq 0$) STBC-NOMA are presented as well.

A. Secrecy Outage Probability

Proposition 1. *For the l-th user, the exact SOP can be expressed as*

$$P_{out,l} = \frac{1}{\left(\lambda_I \lambda_{Ie} \lambda_e\right)^2} Q_l \underset{i,m,n}{\Xi} \left[\left(\lambda_0 \rho\right)^{-n} \mathfrak{E}_p\left(\Delta_l\right)\right]. \tag{5}$$

where $Q_l = L!/(L-l)!(l-1)!$, $\underset{i,m,n}{\Xi}(\Delta) = \sum_{i=0}^{L-l} \frac{(-1)^i \binom{L-l}{i}}{l+i} \sum_{m=0}^{l+i} \binom{l+i}{m} (-1)^m \sum_{n=0}^{m} \binom{m}{n} \Delta$ and Δ_l is the transfer function defined as (A.4).

Proof. The secrecy rate of the l-th LU is defined as [4] $C_l = \max\{0, [\log_2\left(1+\gamma_l\right) - \log_2\left(1+\gamma_{E_l}\right) - R_l]\}$. Given a secrecy rate threshold R_l, the SOP of LU$_l$ can be written as:

$$\begin{aligned} P_{out,l} &= \Pr\left\{1+\gamma_l \leq 2^{R_l}\left(1+\gamma_{E_l}\right)\right\} \\ &= \int_0^\infty F_{\gamma_l}\left(2^{R_l}\left(1+x\right) - 1\right) f_{\gamma_{E_l}}(x) dx, \end{aligned} \tag{6}$$

where $F_X(\cdot)$ and $f_X(\cdot)$ denote the cumulative distribution function (CDF) and probability density function (PDF), respectively. The details of $F_{\gamma_l}\left(\cdot\right)$ and $f_{\gamma_{E_l}}\left(\cdot\right)$ are explained in Appendix A.

$$\begin{aligned} F_{\gamma_l}\left(\xi\right) = \frac{Q_l}{\lambda_I^2} \underset{i,m,n}{\Xi} \Bigg\{ &\exp\left(-\frac{m\delta_l\left(\xi\right)}{\lambda_0 \rho}\right) \left(\frac{\delta_l\left(\xi\right)}{\lambda_0 \rho}\right)^n \\ &\times \mathfrak{E}_p\left[\left(\frac{\lambda_0 \lambda_I}{\lambda_I m w \delta_l(\xi) + \lambda_0}\right)^{p+2}\right] \Bigg\}, \end{aligned} \tag{7}$$

where $\xi < \frac{a_l}{\varepsilon_l}$, $\varepsilon_l = \sum_{k=l+1}^{L} a_k$, $\varepsilon_0 = 1$ for $l = 1$. It is noted that when $l = 1$, $w = 0$ and $p = 0$. $\delta_l\left(\xi\right) = \frac{\xi}{a_l - \varepsilon_l \xi}, 1 < l < L$, $\delta_L\left(\xi\right) = \frac{\xi}{a_L}$, and $\mathfrak{E}_p(x) = \sum\limits_{p=0}^{n} \binom{n}{p} (w\rho)^p \left(p+1\right)!(x)$, and

$$f_{\gamma_{E_l}}\left(\xi\right) = \Im_l\left(\xi\right) \frac{\exp\left(-\frac{1}{\lambda_e \rho_e}\delta_l\left(\xi\right)\right)}{\lambda_{Ie}^2 \lambda_e^2}, \tag{8}$$

[1] Notations: Vectors and matrices are represented by boldface lower case letters and boldface capital letters, respectively, and $[\cdot]^{\mathsf{T}}$ represents the conjugate transposition.

where $\Im_l(\xi)$ is a transfer function defined in (A.3).

By substituting (7) and (8) into (6), the SOP of LU$_l$ can be obtained as (5).

□

Remark 1. *When $l < L$, the Gaussion-Chebshev approximation can be utilized to get the result further,* (6) *can be calculated in* **Lemma** 1.

Lemma 1. The exact SOP when $l < L$.

$$P_{out,l} = \frac{\mathcal{A}\pi}{2U}\sum_{u=1}^{U}\mathcal{S}(u)G\left(\frac{\mathcal{A}(\tau_u+1)}{2}\right)+\mathfrak{F}(\mathcal{A}), \tag{9}$$

where U is a parameter to ensure a complexity-accuracy tradeoff $\mathcal{S}(u)=\sqrt{1-{\tau_u}^2}$ and $\tau_u=\cos\left(\frac{2u-1}{2U}\pi\right)$.

Proof. When $l < L$ the SOP can be directly obtained from (6) as:

$$P_{out,l} = \int_0^{\mathcal{A}} F_{\gamma_l}[\mathcal{B}(x)]\,f_{\gamma_{E_l}}(x)\,dx+\mathfrak{F}(\mathcal{A}), \tag{10}$$

where $\mathcal{A}=\frac{\varepsilon_{l-1}}{\varepsilon_l\theta_l}-1$, $\mathcal{B}(x)=\theta_l-1+\theta_l x$, $\theta_l=2^{R_l}$ and $\mathfrak{F}(x)=1-F_{\gamma_{E_l}}(x)$. Let $G(x)=F_{\gamma_l}[\mathcal{B}(x)]\,f_{\gamma_{E_l}}(x)$, then (10) can be expressed as (9). □

Remark 2. *For $l = L$, which means that* LU$_L$ *has been allocated the smallest transmission power. It will not suffer from other stronger user's interference when decoding the signal of itself, which make the CDF of γ_L and PDF of $\gamma_{E\,L}$ are different with that of γ_l in (7) and (8).*

Lemma 2. The exact SOP when $l = L$. *The approximation of Δ_L in (5) can be written as follows:*

$$\Delta_L \approx \sum_{v=1}^{V}\omega_v f(\xi_v). \tag{11}$$

The SOP expression of LU$_L$ *can be easily obtained by substituting* (11) *into* (5).

Proof. In order to obtain the exact value of Δ_L from (A.4), the Gauss-Laguerre quadrature of $\int_0^\infty f(x)e^{-x}dx \approx \sum\limits_{v=1}^{V}\omega_v f(x_v)$ [14] can be used to get the approximation result of (A.4) when $l = L$, where, the weight of ω_v and points of x_v can be obtained from [14]. Therefore, in order to utilise the Gauss-Laguerre quadrature, based on (A.4)

$$\begin{aligned} f(\xi) = {} & [\delta_L\mathcal{B}(\xi)]^n\,\Im_L(\xi)\left(\frac{\lambda_0\lambda_l}{\lambda_l m\omega\delta_L\mathcal{B}(\xi)+\lambda_0}\right)^{p+2} \\ & \times\exp\left(\xi-\frac{m\delta_L\mathcal{B}(\xi)}{\lambda_0\rho}+\frac{\delta_L}{\lambda_e\rho_e}\right) \end{aligned} \tag{12}$$

Then, the approximation result of Δ_L can be obtained from the Gauss-Laguerre quadrature. □

B. Asymptotic Analysis

In this section, the asymptotic secrecy outage performance of STBC-NOMA is investigated to gain more insights into the system performance in the high SNR regime. The asymptotic performance is investigated as the SNR of the channels between the BS and LUs are sufficiently high, i.e., $(\rho\to\infty)$ and the SNR of the channel between the BS and Eve maintain arbitrary value of ρ_e. And the secrecy diversity order can be expressed as $d=-\lim\frac{\log(P^{\infty}_{out,l}(\rho))}{\log\rho}$.

Lemma 3. Asymptotic SOP of the l-th $(1 < l < L)$ user.

The asymptotic expression of the SOP of LU$_L$ *is:*

$$P^{\infty}_{out,l} = \frac{\mathcal{A}\pi}{2U\varepsilon_l\theta_l}\sum_{u=1}^{U}\mathcal{S}(u)G^{\infty}\left(\frac{(\mathcal{A}+1)\tau_u}{2\varepsilon_l\theta-l}\right)+\mathfrak{F}\left(\frac{\mathcal{A}}{\varepsilon_l\theta_l}\right). \tag{13}$$

Proof. According to (7), when the transmit $\rho\to\infty$, the asymptotic expression of F_{γ_l} can be written as follows:

$$\begin{aligned} F^{\infty}_{\gamma_l}(\xi) = {} & \frac{Q_l}{\lambda_I^2}\underset{i,m,n}{\Xi}\left\{\left(1-\frac{m\delta_l(\xi)}{\lambda_0\rho}\right)\left(\frac{\delta_l(\xi)}{\lambda_0\rho}\right)^n\right. \\ & \left.\times\,\mathfrak{E}_p\left[\left(\frac{\lambda_0\lambda_I}{\lambda_I m w\delta_l(\xi)+\lambda_0}\right)^{p+2}\right]\right\}, \end{aligned} \tag{14}$$

Then, from (9) and (14), let $G^{\infty}(x)=F^{\infty}_{\gamma_l}[\mathcal{B}(x)]\,f_{\gamma_{E_l}}(x)$, the SOP is (13). □

Lemma 4. Asymptotic SOP probability of the 1st user.

The asymptotic expression of the SOP of LU$_1$ is:

$$P^{\infty}_{out,1} = \frac{\pi\mathcal{C}\sum_{u=1}^{U}\mathcal{S}(u)G^{\infty}\left(\frac{(\tau_u+1)\mathcal{C}}{2}\right)}{2U}+\mathfrak{F}(\mathcal{C}). \tag{15}$$

Proof. According to (7), when the transmit SNR approaches ∞, the asymptotic expression of F_{γ_1} can be written as follows when $\xi<\frac{a_1}{\varepsilon_1}$:

$$F^{\infty}_{\gamma_1}(\xi) = Q_1\underset{i,m,n}{\Xi}\left[\left(\frac{\delta_l(\xi)}{\lambda_0\rho}\right)^n\left(1-\frac{m\delta_l(\xi)}{\lambda_0\rho}\right)\right]. \tag{16}$$

Then, the SOP asymptotic expression for LU$_1$ can be obtained by (15). □

Lemma 5. Asymptotic SOP probability of the L-th user.

The asymptotic SOP of the L-th user can be calculated as:

$$P^{\infty}_{out,L} \approx \frac{Q_L}{{\lambda_I}^2{\lambda_{Ie}}^2{\lambda_e}^2}\underset{i,m,n}{\Xi}\left[(\lambda_0\rho)^{-n}\mathfrak{E}_p\left(\Delta^{\infty}_L\right)\right]. \tag{17}$$

Proof. Let $g(\xi)=\left(1-\frac{m\xi}{\lambda_0\rho a_L}\right)\left(\frac{\mathcal{A}}{a_L}\right)^n\left(\frac{a_L\lambda_0\lambda_I}{mw\lambda_I\mathcal{A}+\lambda_0 a_L}\right)^p\Im_L(\xi)$ and $\zeta = 1/\lambda_e\rho_e a_L$, from (A.4), when $\rho\to\infty$, the approximation of Δ^{∞}_L is:

$$\Delta^{\infty}_L = \int_0^{\infty}\exp(\xi\zeta)\,g(\xi)\,\mathrm{d}\xi \approx \frac{1}{\zeta}\sum_{v=1}^{V}\omega_v g(\xi_v), \tag{18}$$

Then the SOP asymptotic expression for LU$_\mathrm{L}$ can be obtained by (17).

The conclusion can be easily obtained that a zero diversity order can be achieved for the nearest user. □

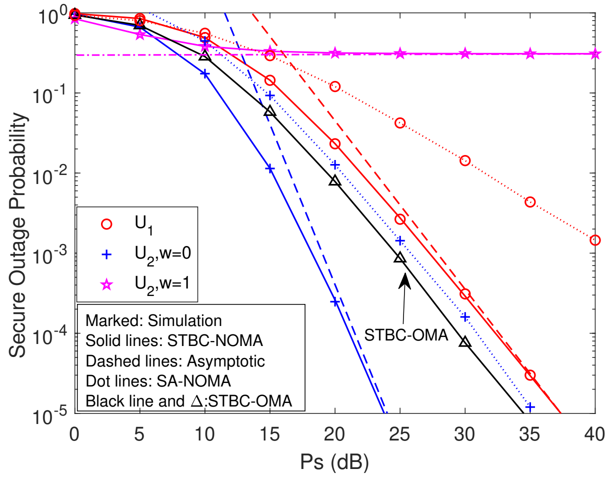

Fig. 1. SOP vs transmit SNR, with $\lambda_0 = 0$ dB.

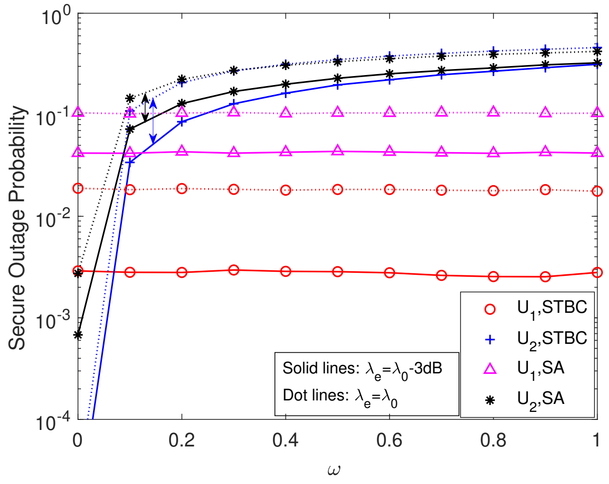

Fig. 2. SOP vs. the imperfect SIC factor ω,with $\rho_s = 20$ dB, $\lambda_0 = 0$ dB.

Remark 3. *Specially, when* $x \to 0$*,* $\tilde{F_X}(x) \approx \frac{1}{2}\left(\frac{x}{\lambda_0}\right)^2$*, we can easily get the ordered CDF of* LU$_L$ *as* $F_{X_l}(x) \approx \frac{Q_L}{L2^L}\left(\frac{x}{\lambda_0}\right)^{2L}$*. The asymptotic SOP of* LU$_L$ *under SIC is:*

$$P^{\infty}_{out,L} = \frac{Q_L}{2^L L \lambda_0^{2L} \lambda_e^2} \sum_{p=0}^{2L} \binom{2L}{p} \left(\frac{\theta_L - 1}{\rho a_L}\right)^p \left(\frac{\theta_L \rho_e}{\rho}\right)^{2L-p} \times (2L+1-p)! \lambda_e^{2-p+2L}, \tag{19}$$

It is noted that the diversity order under pSIC case for all users can be achieved by:

$$P^{\infty}_{out,l} \propto \sum_{i=0}^{L-l} \left(\frac{1}{\rho}\right)^{2(l+i)}. \tag{20}$$

IV. Numerical Results and Analysis

In this section, two LUs ($L = 2$)[2] and one Eve are set as an example for illustrating the numerical results. The power allocation coefficients are set as $a_1 = 0.8$, $a_2 = 0.2$ and target data rates are $R_1 = 0.1$ bit per channel use (BPCU) and $R_2 = 0.2$ BPCU for two LUs. The other parameters are U=20, V=100. Generally, the channel conditions of the legitimate link is considered better than the eavesdropping link. For the numerical analysis, the channel SNR of λ_0 is 3 dB bigger than λ_e. Additionally, the condition that $\lambda_0 = \lambda_e$ is analysed as a specially matched case as well. Similarly, the self-interference channel condition is also deemed to be worse than the legitimate link. The difference is 3 dB for numerical analysis. It is needed to notice that the SNR of the channel between the BS and Eve should be an arbitrary value of ρ_e. Here, as an exmple to illustrate the advantages of STBC-NOMA, ρ_e is set as 10 dB [2]. The conventional Alamouti-OMA (STBC-OMA) and the conventional NOMA (SA-NOMA) are selected to be benchmark for comparing.

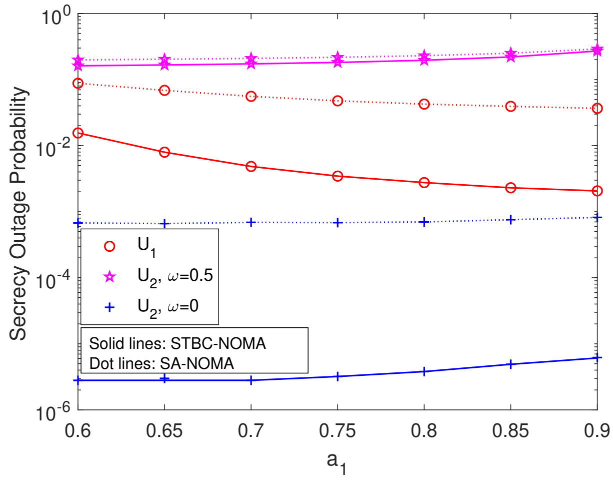

Fig. 3. SOP vs. power allocation coefficient of a_1, with $\rho_s = 25$ dB and $\lambda_0 = 0$ dB.

The SOPs for pSIC ($w = 0$) and ipSIC ($w = 1$) with different values of SNR is presented in Fig. 1. It can be seen that the theoretical results (solid line) match the simulations (marks) well and asymptotic curves (dash line) are tightly convergent to those of exact results in the high SNR regime. The SOP of U$_2$ with ipSIC converge to an error floor and thus gain a zero diversity order. It is also observed that the SOP of U$_2$ with pSIC in STBC-NOMA is superior to that of STBC-OMA due to the SIC technique. Generally, the SOPs of users in the STBC-NOMA are superior than SA-NOMA because of that space time diversity can achieve the extra diversity gain. For example, U$_1$ provides approximately 10 dB SNR gain compared STBC-NOMA to SA-NOMA when the SOP value is 10^{-2}. However, U$_2$ can not obtain any gain under ipSIC case. In Fig. 2, the SOPs for ipSIC factors (ω from $0 \to 1$) under different channel conditions are presented as two cases. *case* 1: $\lambda_e = \lambda_0$ the average SNR of legitimate link equals to that of eavesdropping link; *case* 2: $\lambda_e = \lambda_0 - 3$ the average SNR of legitimate link is 3 dB less than that of

[2] When $L > 2$, the numerical results of STBC-NOMA still match our theoretical inference. In this letter, we propose to verify our algorithm of STBC-NOMA by presenting numerical results when $L = 2$.

eavesdropping link. Obviously, STBC-NOMA can enhance the performance of SOP compared with SA-NOMA because of the extra transmit diversity gain by STBC-NOMA. The gap between the blue solid line and blue dot line is bigger than it between the black lines which means that the SOP of U_2 varies more obviously under *case* 2 than that of *case* 1.

Fig. 3 plots the SOPs versus power allocation coefficient of a_1, where $a_2 = 1-a_1$. It can be seen that the SOP performance of U_1 is enhanced with the increase of the power allocation a_1 from 0.6 to 0.9, which is more obvious by STBC-NOMA compared with SA-NOMA. Secondly, the SOP of U_2 will not increase with the increase of a_1. Furthermore, if the interference cannot be cancelled perfectly (ipSIC with $\omega = 0.5$), STBC-NOMA provides a little better SOP performance than SA-NOMA for U_2 .

V. CONCLUSION AND FURTHER WORK

In this letter, the secrecy outage performance (SOP) of a STBC-NOMA network is analysed. The exact and asymptotic expressions of SOP are derived. The numerical and simulation results show that the STBC-NOMA generally enhances the SOP performance compared with SA-NOMA and STBC-OMA. It should be noted that power allocation optimization between NOMA users with an artificial noise-aided scheme is capable of further improving the secrecy performance of wireless networks, which appears to be promising future research.

APPENDIX A
PROOF OF OUTAGE PROBABILITY FUNCTION

Let $X_l = \|\mathbf{h}_l\|_F^2$, $\psi = \|\mathbf{h}_I\|_F^2$, $\psi_e = \|\mathbf{h}_{Ie}\|_F^2$, $Y = \|\mathbf{h}_e\|_F^2$ Then the CDF and PDF of unordered form of X_l is $\tilde{F}_X(x) = 1 - \exp\left(-\frac{x}{\lambda_0}\right)\sum_{i=0}^{1}\left(\frac{x}{\lambda_0}\right)^i\frac{1}{i!}$ and $\tilde{f}_X(x) = \frac{x}{\lambda_0^2}e^{-\frac{x}{\lambda_0}}$, respectively. The CDF of ordered X_l is $F_{X_l}(x) = Q_l\sum_{i=0}^{L-l}\frac{(-1)^i\binom{L-l}{i}}{l+i}\left(\tilde{F}_X(x)\right)^{l+i}$. By using binomial expansion, it can be calculated as:

$$F_{X_l}(x) = Q_l\sum_{i=0}^{L-l}\frac{(-1)^i\binom{l+i}{m}}{l+i}\sum_{m=0}^{l+i}\binom{L-l}{i}(-1)^m \times\sum_{n=0}^{m}\binom{m}{n}\frac{x^n}{\lambda_0^n}e^{-\frac{mx}{\lambda_0}}, \tag{A.1}$$

where $Q_l = L!/(L-l)!(l-1)!$. Let $\underset{i,m,n}{\Xi}(\Delta) = \sum_{i=0}^{L-l}\frac{(-1)^i\binom{L-l}{i}}{l+i}\sum_{m=0}^{l+i}\binom{l+i}{m}(-1)^m\sum_{n=0}^{m}\binom{m}{n}\Delta$, based on (1), the CDF of F_{γ_l} can be easily obtained and is shown in (7).

Similarly, the CDF of γ_{E_l} is:

$$\begin{aligned} F_{\gamma_{E_l}}(\xi) &= \int_0^\infty F_Y\left(\frac{(1+w\rho_e\varphi)\xi}{\rho_e(a_l-\varepsilon_l\xi)}\right)f_{\psi_e}(\varphi)\,d\varphi \\ &= \frac{1}{2\lambda_{Ie}} - \frac{e^{-\frac{\delta_l(\xi)}{\lambda_e\rho_e}}}{{\lambda_{Ie}}^2}\left[\left(1+\frac{1}{\lambda_e\rho_e}\delta_l(\xi)\right)\left(\frac{w}{\lambda_e}\delta_l(\xi)+\frac{1}{\lambda_{Ie}}\right)^{\text{-2}} \right. \\ &\left. + \frac{2w\delta_l(\xi)}{\lambda_e}\left(\frac{w}{\lambda_e}\delta_l(\xi)+\frac{1}{\lambda_{Ie}}\right)^{\text{-3}}\right], \end{aligned} \tag{A.2}$$

where $\xi < \frac{a_l}{\varepsilon_l}$. Then, from (A.2), the PDF of $F_{\gamma_{E_l}}$ as shown in (8), where,

$$\begin{aligned} \Im_l(\xi) = {\delta_l}'(\xi)\left(\frac{\lambda_e\lambda_{Ie}}{\omega\lambda_{Ie}\delta_L(\xi)+\lambda_e}\right)^2\left[\frac{\delta_l(\xi)}{\rho_e^2} + \frac{2w}{\rho_e}(1+\delta_l(\xi)) \right. \\ \left. \times\left(\frac{\lambda_e\lambda_{Ie}}{\omega\lambda_{Ie}\delta_L(\xi)+\lambda_e}\right) + 6w^2\delta_l(\xi)\left(\frac{\lambda_e\lambda_{Ie}}{\omega\lambda_{Ie}\delta_L(\xi)+\lambda_e}\right)^2\right], \end{aligned} \tag{A.3}$$

where $\delta_l'(\xi) = a_l/(a_l-\varepsilon_l\xi)^2$ when $l < L$ and $\delta_L'(\xi) = 1/a_L$.

By combining (6), (7) and (8), the security outage probability of LU_l is shown in (5). where,

$$\begin{aligned} \Delta_l = \int_0^\infty \exp\left(-\frac{m\delta_l(\xi)\mathcal{B}(\xi)}{\lambda_0\rho} + \frac{\delta_l(\xi)\,(\xi)}{\lambda_e\rho_e}\right)(\delta_l\mathcal{B}(\xi))^n \\ \times\left(\frac{\lambda_0\lambda_I}{\lambda_I mw\delta_l\mathcal{B}(\xi)+\lambda_0}\right)^{p+2}\Im_l(\xi)\,d\xi. \end{aligned} \tag{A.4}$$

REFERENCES

[1] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, H. V. Poor *et al.*, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, 2017.

[2] 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 Trans. on Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, 2017.

[3] W. Wu, F. Zhou, R. Q. Hu, and B. Wang, "Energy-efficient resource allocation for secure noma-enabled mobile edge computing networks," *IEEE Trans. Commun.*, 2019.

[4] X. Yue, Y. Liu, Y. Yao, X. Li, R. Liu, and A. Nallanathan, "Secure communications in a unified non-orthogonal multiple access framework," *arXiv preprint arXiv:1904.01459*, 2019.

[5] H. Lei, J. Zhang, K.-H. Park, P. Xu, Z. Zhang, G. Pan, and M.-S. Alouini, "Secrecy outage of max–min tas scheme in MIMO-NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6981–6990, 2018.

[6] H. Sun, F. Zhou, R. Q. Hu, and L. Hanzo, "Robust beamforming design in a noma cognitive radio network relying on swipt," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 1, pp. 142–155, 2019.

[7] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative miso-noma using swipt," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 918–931, 2018.

[8] J. Choi, "Non-orthogonal multiple access in downlink coordinated two-point systems," *IEEE Commun. Lett.*, vol. 18, no. 2, pp. 313–316, 2014.

[9] M. F. Kader and S. Y. Shin, "Cooperative relaying using space-time block coded non-orthogonal multiple access," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 5894–5903, 2016.

[10] Z. Tang, J. Wang, J. Wang, and J. Song, "Harvesting both rate gain and diversity gain: Combination of noma with the alamouti scheme," in *2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, June 2017, pp. 1–3.

[11] M. Toka and O. Kucur, "Non-orthogonal multiple access with Alamouti space–time block coding," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1954–1957, 2018.

[12] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, 1978.

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

[14] F. B. Hildebrand, *Methods of applied mathematics*. Courier Corporation, 2012.