IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 October 2022, accepted 20 November 2022, date of publication 5 December 2022,
date of current version 15 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3226691

RESEARCH ARTICLE

The 5G Cellular Downlink V2X Implementation Using V2N With Spatial Modulation

WON MEE JANG, (Member, IEEE)
Department of Electrical and Computer Engineering, University of Nebraska–Lincoln, Omaha, NE 68182, USA
e-mail: wjang1@unl.edu

ABSTRACT Fifth generation (5G) New Radio (NR) technology provides cellular vehicle-to-everything (C-V2X) communication. The 5G NR will utilize the existing uplink (UL) and downlink (DL) to furnish vehicle-to-network (V2N) communication via the cellular network. The new technology provides the enhanced throughput, edgeless connectivity, high reliability and the reduced latency for 5G DL V2X. With significantly reduced latency of NR, this paper shows that C-V2X can be implemented via 5G V2N communication. Spatial modulation is a good candidate to support unicast and groupcast for V2X services. We also discuss keyless security of 5G NR using physical layer security. The security of 5G NR can be implemented employing spatial modulation (SM) for unicast and groupcast in millimeter-wave (mmWave) communications with multiple-input and multiple-output (MIMO) channels.

INDEX TERMS 5G new radio, physical layer security, cellular-V2X (C-V2X), spatial modulation (SM), multiple-input and multiple-output (MIMO), mmWave communications.

I. INTRODUCTION

Cellular vehicle-to-everything (C-V2X) is established by the 3rd generation partnership project (3GPP) as part of its long-term evolution (LTE) and subsequently fifth generation (5G) families of standards. The universal mobile telecunications systems (UMTS) developed by the 3GPP specifies a complete network system, which include the radio access network, the mobile application core network, and the authentication. C-V2X is one of the most rapidly growing areas in wireless communication. C-V2X is defined as follows: device-to-network communication i.e. vehicle-to-network (V2N) uses the conventional cellular links including a cloud service as a part of the end-to-end services. On the other hand, device-to-device communication consists of vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle-to-pedestrian (V2P). However, we show that device-to-device communication can be successfully implemented via C-V2X. Since C-V2X operates through cellular networks, a large part of the physical infrastructure is already established. In addition, 5G new radio (NR) can support strict 1 ms latency target, thanks to its flexible numerology [1]. Widely established cellular infrastructure and significantly reduced latency enable V2V, V2I, and V2P using V2N. Additionally adopting C-V2X is relatively cost-effective since both PC5 and user equipment to the UMTS (Uu) interface can be easily integrated into a single C-V2X chipset [2]. However, there are many issues that need to be solved to make the C-V2X communication more successful. The large amount of sensor data is communicated among vehicles, pedestrians, and other road users in a vehicular environment with extremely low latency and high reliability to provide a holistic view of the circumstance in each vehicle. The holistic view enables any perception, planning, and control in road users. Remote driving is generally useful for driving in areas with routine operations of roads such as bus lines in public transportation. In fact, a bus can be driven through a cloud. Advanced driving is mostly for fully or semiautomated driving where vehicles exchange their local sensing information with each other and a road side unit (RSU). Collision avoidance, safer driving, and improved traffic efficiency are some of the benefits of such use case [3].

All the potentials of C-V2X are focused on its second mode, V2N mode. V2N utilizes a cellular network communications interface such as the Uu interface, which coordinates broadcast communication via existing cellular mobile

The associate editor coordinating the review of this manuscript and approving it for publication was Fang Yang.

networks. The ability to connect to the cellular network is a critical feature that wireless local-area network (WLAN)-based direct short-range communication (DSRC) technology cannot furnish. Most urban areas already have LTE-capable cell towers and are being upgraded into 5G cellular infrastructure. If we need the technology to provide internet connections for smartphones and internet of things (IoT), we can just use it for vehicles. C-V2X includes two modes: longer-range, higher latency communication via the cellular network known as C-V2N, and low latency, direct communication referred to as C-V2V/I/P [2].

NR-V2X Rel-16 first defined NR sidelink (SL) with a focus on V2X enhancing the reliability, latency, capacity, and flexibility. SL has the same structure for radio frames, subframes, and slots as NR uplink (UP) and downlink (DL) [4]. SL positioning was specified for multiple V2X and public safety use cases with accurate positioning requirements. For example, relative longitudinal position accuracy of less than 0.5 m for user equipments (UEs) is required in a platooning use case [5]. The radio resources in NR are defined in time and frequency domains. SL communication also supports different numerologies which result in shorter slot times. It is demonstrated that both NR and LTE-advanced can fulfill 5 ms latency target with 99.999% reliability. However, only NR can support even stricter 1 ms latency target [1]. It is an enabling feature to fulfill a low latency requirement. The total capacity of 5G V2I links is maximized while guaranteeing the strict transmission delay and reliability constraints of V2V links using a multi-agent double deep Q-learning algorithm [6]. With the reduced latency, 5G V2N can be implemented for V2X. In 5G C-V2X connectionless groupcast (multicast) mode, groups can form on-the-fly for exchanging messages with little to no overhead for group formation and dismantling. Different cast types such as unicast and groupcast are also specified for V2X communication in addition to broadcast [3]. In this paper, we show that spatial modulation can be used in 5G cellular DL to support unicast and groupcast in a platooning traffic flow.

Space shift keying (SSK) is a transmission method of multiple-input multiple-output (MIMO) systems. With SSK, the information is carried with transmit antenna indices. On the other hand, spatial modulation (SM) transmits data using inphase and quadrature (IQ) modulation in addition to antenna indices. Conventional SSK was presented in [7], [8], [9], [11], and [10] where only one transmitter transmits a signal at a time while the others are inactive. A variant of SSK for radio communication was reported in [12] and [13] where more than one antenna transmits data over each time instant. This leads to the concept of generalized space shift keying (GSSK). GSSK is therefore a special form of SSK [14], [15]. The space-time coding (STC) concept of space-time shift keying (STSK) provides a flexible tradeoff between the achievable diversity gain and the throughput [16]. The error performance analysis of a low complexity, multiple transmitter GSSK signaling technique was presented for short range indoor visible light communications [17], [18], [19].

Receiver space shift keying (RSSK) utilizes receive antenna indices for data transmission [20], [21]. In fact, RSSK outperforms transmit space shift keying (TSSK) under the same transmit power and signal bandwidth in DL cellular systems. TSSK is generally known as SSK in the literature. Therefore, when there is a larger number of transmit antennas than receive antennas, receiver spatial modulation (RSM) can perform better than TSSK while maintaining the same data rate. TSSK requires maximum-ratio combining (MRC) at the receiver. On the other hand, RSM needs channel state information (CSI) at the transmitter to perform maximum-ratio transmission (MRT).

Secure communications in the presence of an eavesdropper have been actively investigated [22]. Interestingly, recent years have witnessed a renewed interest in information-theoretic security — widely accepted as the strictest notion of security — which calls for the use of physical-layer techniques that exploit the inherent randomness of the communication medium to guarantee both reliable and secure communication between legitimate parties [23]. Information-theoretic security, based on Shannon's secrecy [24], was laid out by Wyner [25], Csiszár, and Körner [26]. Since then, secrecy capacity has been one of the most important areas of research [27], [28], [29], [30], [31], [32]. Secrecy capacity has been successfully integrated in an MIMO system [33], [34], [35], [36], [37]. The physical layer secrecy of MIMO wireless communication has received extensive attention. The semidefinite relaxation precoding technique was studied and applied in an MIMO system to minimize the transmission power with a certain secrecy channel capacity [38]. Secure signaling over an MIMO wiretap channel was also studied under interference and transmit power constraints [39]. In addition, the secrecy rate maximization problem was studied for an MIMO secrecy channel, where a multi-antenna cooperative jammer was employed to improve secret communication in the presence of multiple multi-antenna eavesdroppers [40].

Massive multiple antenna systems combined with millimeter-wave (mmWave) communication have attracted tremendous interest due to their high data transmission rate. One of the major factors of 5G networks, at the physical layer, is heterogeneous cellular networks (HetNets) with massive MIMO technology and mmWave communication at 10 GHz to 300 GHz radio frequency (RF) bands with bandwidths as high as 2 GHz [41], [42], [43]. As a result, HetNets create an overlay deployment layer of small cells of low-powered base stations, variable communication ranges, and operating frequencies on existing sub-6 GHz macro cells, thus, providing enhanced coverage and throughput to end users by bringing network closer to them [44], [45]. However, it was observed that the higher directivity gain at mmWave cells leads to a drop in the network's secrecy performance; thus, a tradeoff exists between coverage and secrecy [44]. Perfect synchronization and DL CSI are often assumed for performance analysis of MIMO secrecy capacity. In time division duplex (TDD) massive MIMO systems, such as 5G,

the DL CSI is available through channel reciprocity via UL channel training. However, an imperfect or outdated CSI can negatively affect system performance, and it has a substantial impact on performance analysis and secrecy capacity [46], [47].

In this paper, we investigate 5G NR V2N implementation of groupcast and unicast using TSSK-MRC and RSM-MRT, respectively. We also explore the keyless secrecy of unicast and groupcast, and demonstrate that the secrecy capacity of RSM-MRT is significantly better than that of TSSK-MRC in DL cellular systems. The result verifies the validity of the implementation of the unicast using RSM-MRT. On the other hand, secrecy capacity vanishes among UEs of groupcast in a platooning case. This fact demonstrates the feasibility of the implementation of the groupcast using TSSK-MRC in DL cellular systems. Alice, at the base station, transmits data to Bob, the legitimate receiver, and Eve acts as an eavesdropper in a unicast system. Meanwhile, every UEs in groupcast acts as Bob and Eve simultaneously and secrecy capacity vanishes among them to share the traffic information as a group. We investigate the implementation of groupcast and unicast using TSSK-MRC and RSM-MRT, respectively, in Section II. Keyless secrecy of unicast and groupcast is discussed in Section III. Section IV presents the numerical results. We conclude the paper in Section V.

SYMBOL NOTATION

Symbol notations used throughout the paper are listed in Table 1.

TABLE 1. Notation Table.

P	Number of transmit antennas
M	Number of receive antennas
$\alpha_{i,j}$	Channel gain of ith antenna to jth antenna
$\mathbf{H}$	Channel matrix
$\mathbf{x}^T$	Transpose of $\mathbf{x}$
E_s	Symbol energy
$\mathbf{x}$	Data vector
$\boldsymbol{\eta}$	Complex noise vector
$\mathbf{h}_j$	jth column of channel matrix $\mathbf{H}$
E_p	Pulse energy
E_b	Bit energy
σ_n^2	Noise variance
σ_{n_b}	Noise standard deviation of Bob
σ_{n_e}	Noise standard deviation of Eve
γ	Bit energy to noise ratio
$\mathbf{H}_b$	Channel matrix of Bob
$\mathbf{H}_e$	Channel matrix of Eve
$\boldsymbol{\eta}_b$	Complex noise vector of Bob
$\boldsymbol{\eta}_e$	Complex noise vector of Eve
$\lvert\cdot\rvert$	Magnitude of the argument
$H(\cdot)$	Mutual information
$I(\cdot)$	Entropy
$E(\cdot)$	Expectation operator
C_T^b	TSSK channel capacity of Bob
C_T^e	TSSK channel capacity of Eve
C_T^s	TSSK secrecy capacity
$\mathbf{s}_T^b$	TSSK position indicator vector of Bob
$\mathbf{s}_T^e$	TSSK position indicator vector of Eve
P_e^b	Error probability of Bob
P_e^e	Error probability of Eve
C_{RSM}^b	RSM channel capacity of Bob
C_{RSM}^e	RSM channel capacity of Eve
C_{RSM}^s	RSM secrecy capacity
$\mathbf{s}_{RSM}^b$	RSM position indicator vector of Bob
$\mathbf{s}_{RSM}^e$	RSM position indicator vector of Eve

II. UNICAST USING RMS-MRT AND GROUPCAST USING TSSK-MRC

3GPP Rel-16 defined three cast types for NR-V2X. The reason to provide more cast types in comparison with LTE-V2X is to satisfy requirements of a wider range of use cases in vehicular networks. The supported cast types in NR-V2X are as follows [3]: (1) Unicast: direct communication between a pair of UEs. (2) Broadcast: a single transmitter UE sends messages to be received by all UEs which may decode the message (within the radio transmission range of the transmitter UE). (3) Groupcast: a transmitter UE sends message(s) to a set of receivers which fulfill certain conditions, e.g., being member of a group. Broadcast communication was the only supported cast type in LTE-V2X which was limiting its use cases to broadcast safety messages such as cooperative awareness message (CAM). However, NR-V2X supports unicast and groupcast for various applications such as platooning and extended sensors. A platoon forms a chain of vehicles that follow each other with a safety distance sustaining a low latency and highly reliable communication among them. The head of a platoon transmits commands and receives feedback from the other members to manage the platoon.

NR-V2X supports hybrid automatic repeat request (HARQ) procedure for unicast and groupcast messages which can furnish more reliability for these traffic types. SL HARQ is an additional property of Rel-16 for NR-V2X to increase the reliability of unicast and groupcast communication using re-transmissions based on a feedback channel. LTE-V2X does not furnish such a feature in SL since it sustains only broadcast communication in SL. Rel-17 NR SL focus on providing lower latency, higher reliability, extended coverage, and reduced power consumption for battery-based UEs for V2X application. In this section, we show that groupcast and unicast can be implemented via 5G cellular DL V2N using TSSK-MRC and RSM-MRT, respectively. NR C-V2N communication system is displayed in Fig. 1. Let us consider SSK in a DL cellular system with P transmit antennas at the base station, and M receive antennas at the mobile station. The channel matrix $\mathbf{H}$ in which the ith row and jth column can be represented as α_{ij}. The symbol α_{ij} is the channel gain from the jth transmit antenna to the ith receive antenna

$$\mathbf{H} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1P} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2P} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_{M1} & \alpha_{M2} & \cdots & \alpha_{MP} \end{pmatrix} \tag{1}$$

where α_{ij} has a complex normal distribution with zero mean and unit variance, $\alpha_{ij} \sim \mathcal{C}(0, 1)$. If we assume that the jth transmit antenna is active, the received vector can be

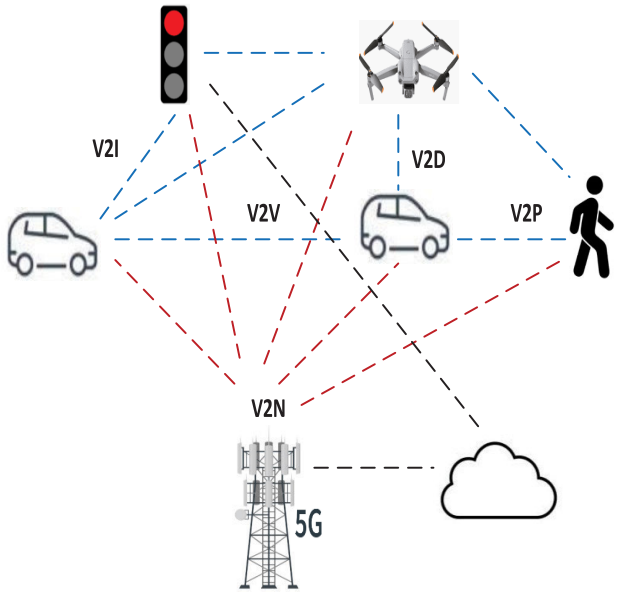


FIGURE 1. 5G NR vehicle-to-network (V2N) services.

shown as

$$\mathbf{y} = [y_1, \ldots, y_M]^T \tag{2}$$
$$= \sqrt{E_s}\mathbf{H}\mathbf{x} + \boldsymbol{\eta} \tag{3}$$
$$= \sqrt{E_s}\mathbf{h}_j + \boldsymbol{\eta} \tag{4}$$

where $\mathbf{h}_j$ is the jth column of $\mathbf{H}$. E_s is the symbol energy. The symbol $\mathbf{x}$ is a random vector, and $\mathbf{x} = [x_1, \ldots, x_P]^T = [0, \ldots 1, \ldots, 0]^T$ where T denotes the matrix transpose. $x_j = 1$ when the jth antenna transmits a signal. $\boldsymbol{\eta}$ is a vector of complex noise with zero mean and variance σ_n^2, i.e., $\eta_m \sim \mathcal{C}(0, \sigma_n)$ for $m = 1, \cdots, M$. With TSSK-MRC, we find

$$\mathbf{z}_T = [z_1, \ldots, z_M]^T \tag{5}$$
$$= \mathbf{H}^\dagger \mathbf{y} \tag{6}$$
$$= \sqrt{E_s}\mathbf{H}^\dagger\mathbf{H}\mathbf{x} + \mathbf{H}^\dagger\boldsymbol{\eta} \tag{7}$$

where the symbol † denotes the Hermitian transpose.

On the other hand, if we employ RSSK-MRT,

$$\mathbf{z}_R = \sqrt{\frac{E_s}{P_{ow}}}\mathbf{H}\mathbf{H}^\dagger\mathbf{x} + \boldsymbol{\eta} \tag{8}$$

where the power scaling factor

$$P_{ow} = \sum_{p=1}^{P} \alpha_{jp}^2 \tag{9}$$

and $x_j = s_l$ and $x_m = 0$ for $m = 1, \cdots, M, m \neq j$ in the data vector $\mathbf{x}$. Hence, the receiver antenna index j indicates the data carrier, and s_l is the data symbol for $l = 1, \cdots L$ for a L-ary signal constellation. Due to the power scaling factor, RSM-MRT maintains the same power as TSSK-MRT.

The RSM-MRT system is shown in Fig. 2 without the power scaling factor for simplicity. The first block IQ modulation modulates the data using in-phase and quadrature

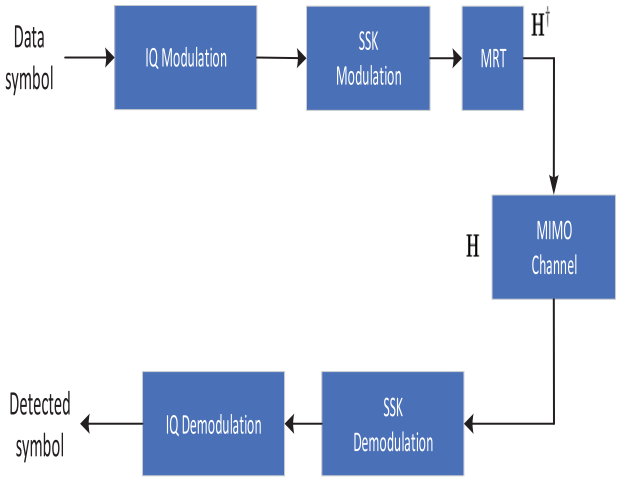


FIGURE 2. Receiver SM system with MRT.

modulation such as BPSK, QPSK, or QAM. The antenna index is determined to carry the spatial information in the second block. The channel state information is fingerprinted on the data vector in the third block. The data is transmitted via the designated antenna through the channel. The lower blocks indicate the receiver operation to undo the corresponding block processes done at the transmitter. Finally, the data symbol is detected and recovered. With RSM-MRT, the receiver output vector can be shown as

$$\mathbf{z}_{RSM} = \sqrt{\frac{E_p}{P_{ow}}}\mathbf{H}\mathbf{H}^\dagger\mathbf{x} + \boldsymbol{\eta}. \tag{10}$$

where E_p is the pulse energy.

The performance of MRC-based SM is obtained in [48]. Using the moment generating function (MGF) [49], the symbol error rate (SER) of TSSK-MRC can be shown as

$$P_s \approx (P-1) \times \left(\frac{1-\mu}{2}\right)^{M-1} \sum_{j=0}^{M-2} \binom{M-2+j}{j} \left(\frac{1+\mu}{2}\right)^j \tag{11}$$

with

$$\mu = \sqrt{\frac{\gamma/4}{1+\gamma/4}} \tag{12}$$

where $\gamma = E_b/\sigma_n^2$, and E_b is the bit energy.

Using the MGF, the SER of RSM-MRT can be shown as [48]

$$P_s \approx \frac{ML-L}{L^2} \times \sum_{l=1}^{L}\left(\frac{1-\mu_1}{2}\right)^{P-1} \sum_{j=0}^{P-2} \binom{P-2+j}{j} \left(\frac{1+\mu_1}{2}\right)^j + \frac{1}{L}\sum_{l=1}^{L}\sum_{\substack{k=1 \\ k\neq l}}^{L}\left(\frac{1-\mu_2}{2}\right)^{P} \sum_{j=0}^{P-1} \binom{P-1+j}{j} \left(\frac{1+\mu_2}{2}\right)^j \tag{13}$$

with

$$\mu_1 = \sqrt{\frac{\gamma|s_l|^2/4}{1+\gamma|s_l|^2/4}} \tag{14}$$

and

$$\mu_2 = \sqrt{\frac{\gamma|s_l - s_k|^2/4}{1+\gamma|s_l - s_k|^2/4}}. \tag{15}$$

III. KEYLESS SECRECY OF UNICAST AND GROUPCAST

Achieving secure vehicular communications is vital for the deployment of V2X applications [50]. Confidentiality and security issues are generally managed in the upper layers of the protocol stack using key-based security encryption techniques. These cryptographic techniques are based on computational mathematical operations, which are difficult for an attacker with limited computational power to perform [50]. The existing 5G-V2V standard permits protection of V2V messages to be dealt by higher layer security solutions specified by other standards in the intelligent transportation system (ITS) domain. However, having a security solutions at the 5G access layer is conceivably preferable in order to ensure system compatibility and reduce deployment cost [2]. In order to improve the issues of the upper layer solutions, some physical layer security (PLS) solutions have been proposed for device-to-device communication to transfer security functions from the upper layer to the lower layer, so as to solve the wireless link security problem. The UE first gathers the physical information and produces the fingerprint parameters which would be served to randomize the parameters used in the authentication and key agreement (AKA) protocol. Subsequently, with the aid of the fingerprint parameters, an enhanced AKA protocol is performed [51].

Information-theoretic results show potentially hiding messages from eavesdroppers or authenticating devices without a shared secret key by designing solutions based on the physical characteristics of the radio channel [50]. PLS is able to facilitate security without any form of encryption in the upper layers. PLS techniques have proven capable of realizing verifiable security even when the network intruders have almost limitless computational resources [52]. Recent advances in quantum computing pose a serious threat to the currently used cryptographic schemes with their unlimited computational capacity [53]. The facilitation of key-free encryption is made possible by the exploitation of some wireless channel characteristics through the application of suitable signaling and channel coding [54]. The basic idea of PLS is to exploit the characteristics of the wireless channel and its impairments including noise, fading, interference, dispersion, diversity, etc., in order to ensure the ability of the intended user to successfully perform data decoding while preventing eavesdroppers from doing so [50], [55]. Thus, the main objective of PLS is to increase the performance difference between the link of the legitimate receiver and that of the eavesdropper by using carefully planned transmission schemes. In the near future, users are expected to be willing to pay extra charges just for the sake of completely ensuring the security of their critical services. Thus, physical security as a service is expected to be one of the future coming killer applications for mobile service providers, where users can be charged a little more for providing them with strong, perfect secure services [55]. The physical layer security solutions can significantly reduce interference and keep eavesdroppers from intercepting communications. The scheme used the direct link transmission and beamforming to achieve a balance between minimizing power and maximizing privacy [51]. In this section, we expand the conceptual and generic PLS framework to NR V2N unicast and groupcast communications.

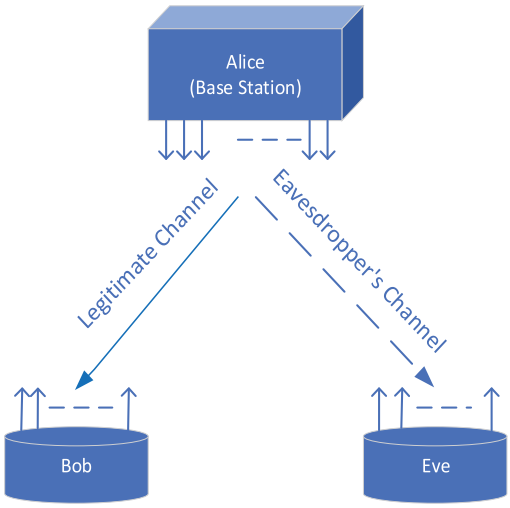


FIGURE 3. Legitimate channel (Alice and Bob) and eavesdropper's channel (Alice and Eve); cellular DL channels.

An MIMO eavesdropper wiretap channel is presented in Fig. 3. Since we are considering DL cellular systems, let us consider Alice located at the base station. Alice transmits a signal to Bob who is the legitimate receiver. Meanwhile Eve who is a third party tries to eavesdrop on Alice's signal. Both Bob and Eve's mobile phones are equipped with the same number of receive antennas. In this paper, we investigate the secrecy capacity for Bob who can safely communicate with Alice with a secrecy rate. Most PLS schemes assume prior knowledge of the eavesdropper's wiretap channel, which is not feasible in practical applications [52]. However, we show that PLS can be safely achieved using RSM-MRT without prior knowledge of Eve's channel characteristics.

a: The secrecy capacity of TSSK with MRC for groupcast

Let us consider the TSSK-MRC with the receiver output of Bob and Eve. The legitimate receiver Bob, and the eavesdropper Eve can afford their own CSI. Therefore, after MRC, $\mathbf{z}_T^b$ and $\mathbf{z}_T^e$ are available to Bob and Eve, respectively. Hence,

$$\mathbf{z}_T^b = \left[z_1^b, \ldots z_P^b\right]^T = \sqrt{E_s}\mathbf{H}_b^\dagger \mathbf{H}_b \mathbf{x} + \mathbf{H}_b^\dagger \boldsymbol{\eta}_b \tag{16}$$

$$\mathbf{z}_T^e = \left[z_1^e, \ldots z_P^e\right]^T = \sqrt{E_s}\mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{x} + \mathbf{H}_e^\dagger \boldsymbol{\eta}_e \tag{17}$$

where $\boldsymbol{\eta}_b$ and $\boldsymbol{\eta}_e$ are independent identically distributed (iid) complex Gaussian random vectors, $\mathcal{C}(0, \sigma_{n_b})$ and $\mathcal{C}(0, \sigma_{n_e})$, respectively. For the numerical results in the following section, we assume $\sigma_{n_b} = \sigma_{n_e} = \sigma_n$. It was observed that the base antennas were nearly uncorrelated at two wavelengths at 2.11 GHz in Manhattan [56]. The result indicates that when Eve is more than 1.42 meters away from Bob, the two channel matrices $\mathbf{H}_b$ and $\mathbf{H}_e$ are independent. A mmWave channel will mostly be line-of-sight (LOS), near LOS, or consist of a single reflected path. The optimum inter-antenna separation that can result in orthogonal channel matrices under LOS conditions is typically of the order of tens of wavelengths. Therefore, $\mathbf{H}_b$ and $\mathbf{H}_e$ become independent if the distance between Bob and Eve is more than 0.1 m and 0.05 m for 28 GHz and 60 GHz, respectively. Therefore, we can safely assume the channel matrices $\mathbf{H}_b$ and $\mathbf{H}_e$ are independent in mmWave communications. The detected symbol can be expressed as

$$\mathbf{s}_T^b = \arg\max_p \{|\mathbf{z}_T^b|\} \tag{18}$$

$$\mathbf{s}_T^e = \arg\max_p \{|\mathbf{z}_T^e|\} \tag{19}$$

$$p = 1, \cdots, P \tag{20}$$

where $|\cdot|$ denotes the magnitude of the argument. The eavesdropper can employ sequential detection. However, a performance improvement of the eavesdropper can be hardly expected due to independent data for each transmission. In addition, when $\mathbf{H}_b$ and $\mathbf{H}_e$ are independent, it eliminates any possibility of eavesdropper's performance improvement. The symbols $\mathbf{s}_T^b$ and $\mathbf{s}_T^e$ are the recovered position indicator vector of the transmit antenna index. Therefore, the capacities of Bob and Eve are

$$C_T^b = E_{\mathbf{H}_b,\boldsymbol{\eta}_b}\left[\max_{P_{\mathbf{X}(x)}} I(\mathbf{x}; \mathbf{s}_T^b|\mathbf{H}_b)\right] \tag{21}$$

$$= E_{\mathbf{H}_b,\boldsymbol{\eta}_b}\left[\max_{P_{\mathbf{X}(x)}} \left\{H(\mathbf{x}) - H(\mathbf{x}|\mathbf{s}_T^b, \mathbf{H}_b)\right\}\right] \tag{22}$$

$$C_T^e = E_{\mathbf{H}_e,\boldsymbol{\eta}_e}\left[\max_{P_{\mathbf{X}(x)}} I(\mathbf{x}; \mathbf{s}_T^e|\mathbf{H}_e)\right] \tag{23}$$

$$= E_{\mathbf{H}_e,\boldsymbol{\eta}_e}\left[\max_{P_{\mathbf{X}(x)}} \left\{H(\mathbf{x}) - H(\mathbf{x}|\mathbf{s}_T^e, \mathbf{H}_e)\right\}\right] \tag{24}$$

where $I(\cdot)$ and $H(\cdot)$ are the mutual information and entropy, respectively. The expectation operation $E[\cdot]$ is over the channel gain matrix and channel noise. It was demonstrated that the full capacity may only be achieved by using equiprobable inputs for a symmetric discrete memoryless channel (DMC) [57, pp. 94], [58]. However, equiprobable inputs may not achieve the full secrecy capacity. Nevertheless, our derivation assumes equiprobable inputs since we investigate the secrecy capacity in practical scenarios of DL cellular systems. Therefore, we can obtain

$$C_T^b = log_2(P) + \left[(1 - P_e^b)log_2(1 - P_e^b) + P_e^b log_2(P_e^b/(P-1))\right] \tag{25}$$

$$C_T^e = log_2(P) + \left[(1 - P_e^e)log_2(1 - P_e^e) + P_e^e log_2(P_e^e/(P-1))\right] \tag{26}$$

where P_e^b and P_e^e are the error probabilities for Bob and Eve, respectively. We assume equiprobable error transition to other symbols due to TSSK-MRC. Secrecy capacity is defined as the rate at which a transmitter can use the main link so as to deliver its message to the legitimate receiver in a way that the eavesdropper cannot successfully decode the same information [59]. The secrecy capacity shows the difference between the capacities of the main and wiretap channels [27]. Therefore, the secrecy capacity can be expressed as

$$C_T^s = C_T^b - C_T^e. \tag{27}$$

We can see that secrecy capacity is afforded only if Bob's channel characteristics are better than Eve's, in other words, $P_e^b < P_e^e$. Under the assumption that $\mathbf{H}_b$ and $\mathbf{H}_e$ have the same distribution, we can expect that Bob can have a positive secrecy capacity when his SNR is superior to Eve's. Therefore, TSSK-MRC is suitable for groupcast, where every member in a group share the same traffic information. It is natural that the secrecy capacity vanishes among each member in groupcast.

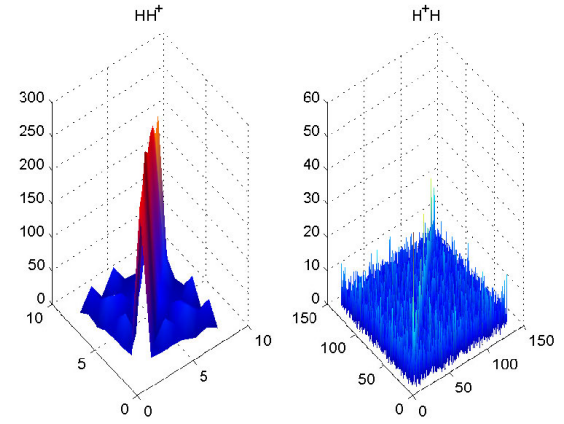
b: Secrecy capacity of RSM with MRT for unicast

We can reasonably assume that Alice in the base station is unaware of the existence of Eve. Hence, Alice knows only her legitimate receiver Bob's CSI. The legitimate receiver Bob and the eavesdropper Eve may afford their own CSI but not the other party's CSI. Bob needs to know his own CSI for the frequency division duplex (FDD) to feedback the CSI to Alice. However, he needs not estimate his CSI for TDD since Alice can monitor the uplink channel from Bob to obtain the CSI. Using RSM-MRT, Bob and Eve can receive $\mathbf{z}_{RSM}^b$ and $\mathbf{z}_{RSM}^e$, respectively:

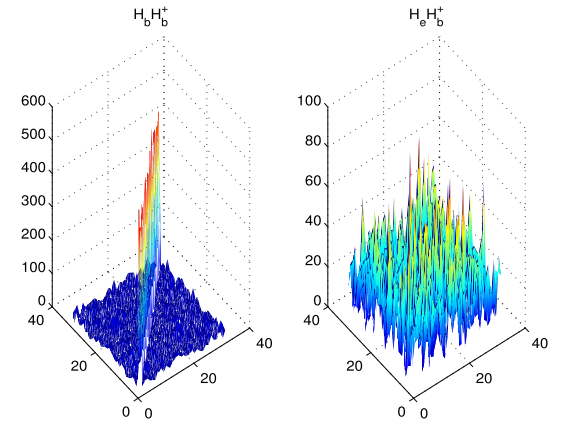
$$\mathbf{z}_{RSM}^b = \sqrt{\frac{E_p}{P_{ow}}}\mathbf{H}_b\mathbf{H}_b^\dagger\mathbf{x} + \boldsymbol{\eta}_b \tag{28}$$

$$\mathbf{z}_{RSM}^e = \sqrt{\frac{E_p}{P_{ow}}}\mathbf{H}_e\mathbf{H}_b^\dagger\mathbf{x} + \boldsymbol{\eta}_e. \tag{29}$$

Fig. 4(a) shows the channel characteristics of TSSK-MRC and RSSK-MRT for DL cellular systems with $P = 128$ and $M = 8$. We can observe that the strong diagonal term of $HH^\dagger$ in RSSK-MRT, which can be effectively traded with IQ modulation. On the other hand, the TSSK-MRC diagonal term is weak, and we can expect that RSSK-MRT significantly outperforms TSSK-MRC at the expense of a reduced data rate. The data rate of TSSK-MRC is $log_2(P)$, while the data rate of RSSK-MRT is $log_2(M)$, and $P \gg M$ in DL cellular systems. To ameliorate the reduced data rate of RSSK-MRT, we employ RSM-MRT with IQ modulation. Fig. 4(b) exhibits the channel characteristics of the legitimate receiver, Bob, and the eavesdropper, Eve, for $P = 256$ and $M = 32$ when

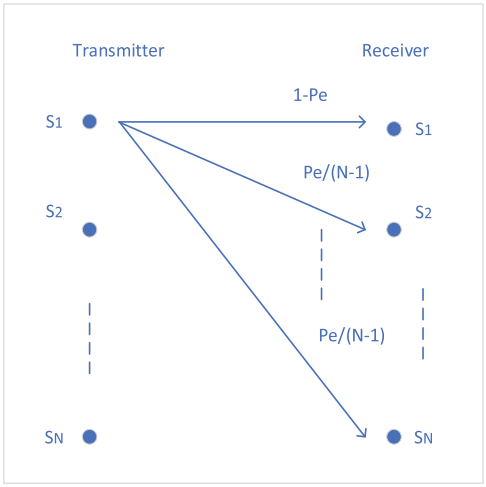


(a) RSSK-MRT ($\mathbf{H}\mathbf{H}^{\dagger}$) and TSSK-MRC ($\mathbf{H}^{\dagger}\mathbf{H}$); $P = 128$, $M = 8$.

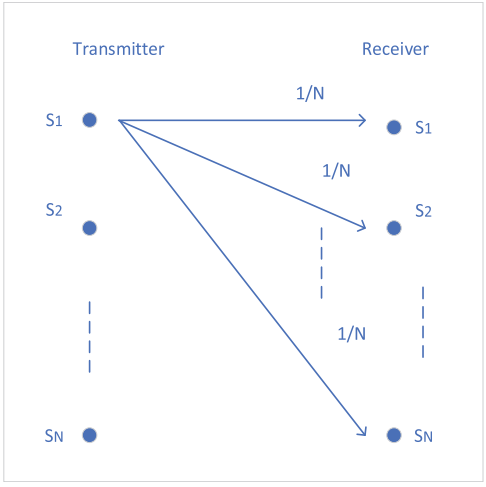


(b) RSM-MRT Bob ($\mathbf{H}_b\mathbf{H}_b^{\dagger}$) and RSM-MRT Eve ($\mathbf{H}_e\mathbf{H}_b^{\dagger}$) ; $P = 256$, $M = 32$.

FIGURE 4. Channel characteristics of (a) RSSK-MRT vs. TSSK-MRC, and (b) RSM MRT Bob vs. RSM MRT Eve.



(a) Channel symbol transition of Bob.



(b) Channel symbol transition of Eve.

FIGURE 5. RSM-MRT channel transition of symbols.

Alice at the base station employs RSM-MRT. We can see that Bob's RSM-MRT channel is significantly superior to Eve's. We observe that there is no diagonal dominance in Eve's RSM-MRT channel. In fact, the eigenvalues of Eve's RSM-MRT channel exhibit singular values, and her symbol error rate (SER) deteriorates rapidly.

Let us consider the channel capacity of Bob and Eve in RSM-MRT in DL cellular systems. The channel capacity of Bob and Eve can be found as [60]

$$C^b_{RSM} = E_{\mathbf{H}_b,\eta_b}\left[\max_{P_{\mathbf{x}(x)}} I(\mathbf{x};\mathbf{s}^b_{RSM}|\mathbf{H}_b)\right] \tag{30}$$

$$= E_{\mathbf{H}_b,\eta_b}\left[\max_{P_{\mathbf{x}(x)}}\left\{H(\mathbf{x}) - H(\mathbf{x}|\mathbf{s}^b_{RSM},\mathbf{H}_b)\right\}\right] \tag{31}$$

$$C^e_{RSM} = E_{\mathbf{H}_b,\mathbf{H}_e,\eta_e}\left[\max_{P_{\mathbf{x}(x)}} I(\mathbf{x};\mathbf{s}^e_{RSM}|\mathbf{H}_e,\mathbf{H}_b)\right] \tag{32}$$

$$= E_{\mathbf{H}_b,\mathbf{H}_e,\eta_e}\left[\max_{P_{\mathbf{x}(x)}}\left\{H(\mathbf{x}) - H(\mathbf{x}|\mathbf{s}^e_{RSM},\mathbf{H}_e,\mathbf{H}_b)\right\}\right] \tag{33}$$

where the symbols $\mathbf{s}^b_{RSM}$ and $\mathbf{s}^e_{RSM}$ denote the recovered transmit antenna index and data symbol for Bob and Eve, respectively. With the assumption of equiprobable inputs, and $N = ML$

$$C^b_{RSM} = log_2(N) + \left[(1-P^b_e)log_2(1-P^b_e) + P^b_e log_2(P^b_e/(N-1))\right] \tag{34}$$

$$C^e_{RSM} = log_2(N) + log_2(1/N) = 0. \tag{35}$$

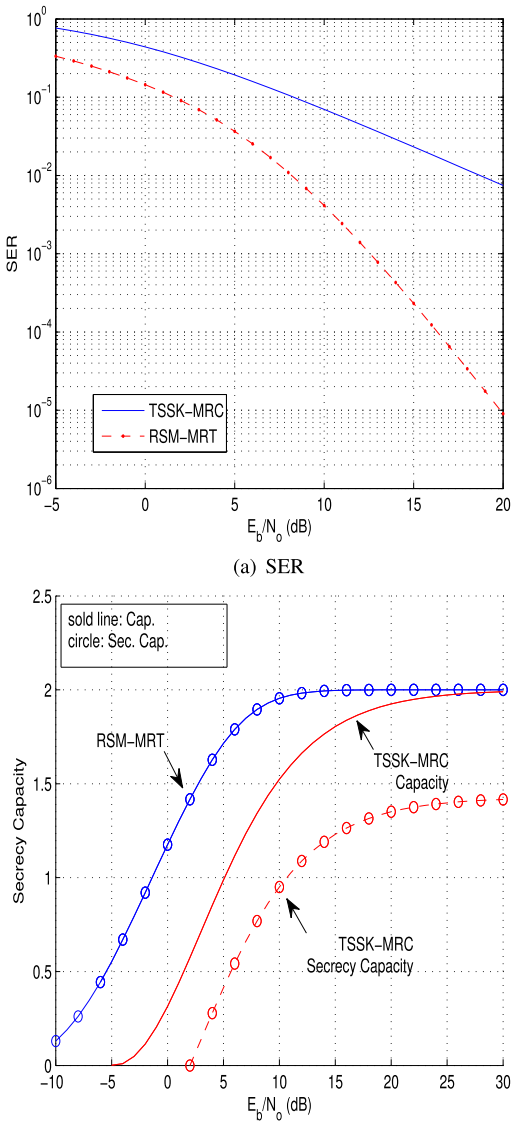
For independent channel matrices, the eigenvalues of $\mathbf{H}_e\mathbf{H}_b^{\dagger}$ are singular, and the channel capacity of Eve vanishes, as shown in (35). The error probability of Bob exhibits the equiprobable transition to other symbols, as shown in Fig. 5(a). On the other hand, Fig. 5(b) shows that the symbol transition of Eve displays a uniform distribution due to the mismatched channel gain matrices. Therefore, the secrecy capacity can be obtained as

$$C^s_{RSM} = C^b_{RSM} - C^e_{RSM} = C^b_{RSM}. \tag{36}$$

As a result, the legitimate receiver achieves the secrecy capacity equal to his isolated single channel capacity using RSM-MRT in DL cellular systems. Therefore, RSM-MRT is

TABLE 2. Simulation parameter settings.

	SSK/SM	P	M	Eve's SNR (dB)	Modulation
Fig. 6	TSSK/RSM	4	2	2	BPSK
Fig. 7	TSSK/RSM	8	2	6	QPSK
Fig. 8	TSSK/RSM	32	2	5	QAM
Fig. 9	TSSK/RSM	4, 8, 32	2	6 -20 to 20	BPSK, QPSK, QAM



(a) SER

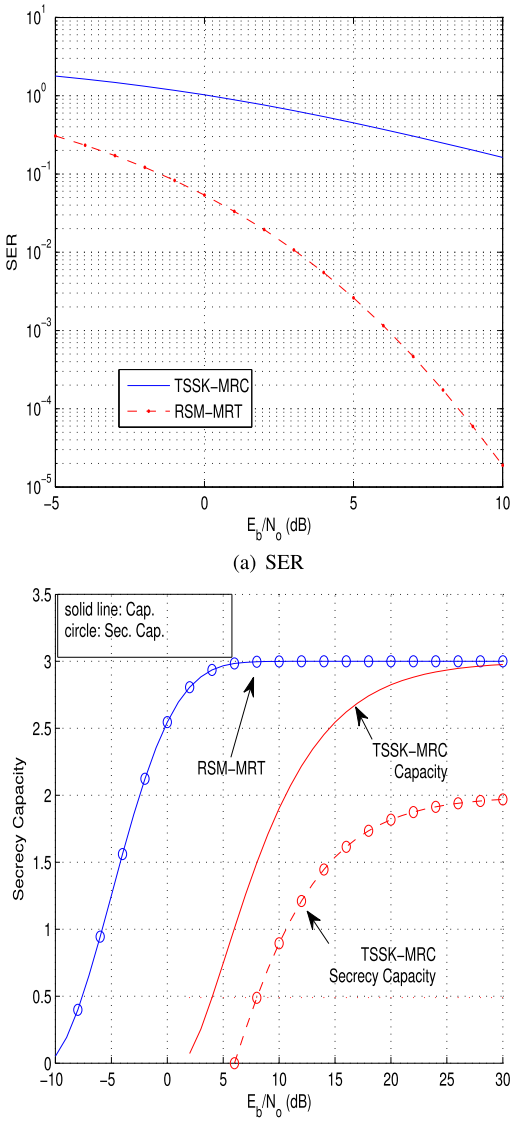
(b) Secrecy Capacity

FIGURE 6. TSSK-MRC, Eve SNR = 2 dB; RSM-MRT with BPSK; $P = 4, M = 2$.

feasible for unicast, where the valid transmitter and receiver pair enjoy the secrecy capacity that is equal to an insolated single user capacity.

IV. NUMERICAL RESULTS

The simulation is performed using MATLAB version 9.8.0.1323502 (R2020a), and the simulation results are

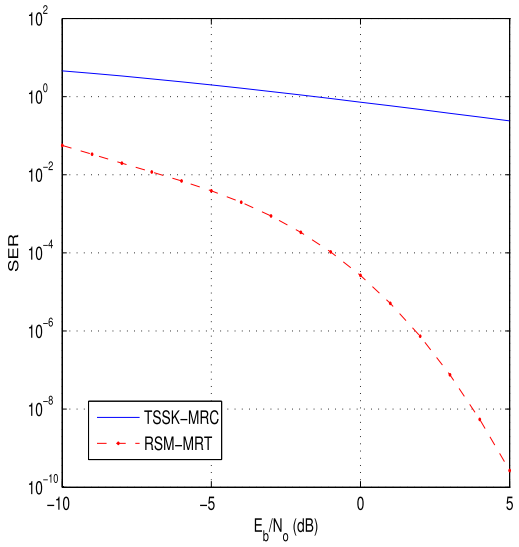


(a) SER

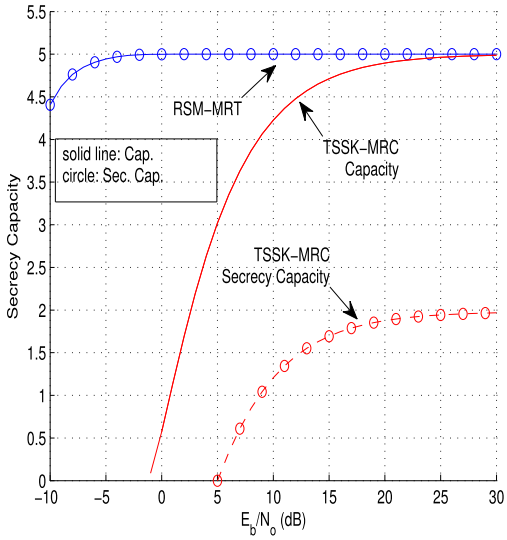
(b) Secrecy Capacity

FIGURE 7. TSSK-MRC, Eve SNR = 6 dB; RSM-MRT with QPSK; $P = 8, M = 2$.

shown in Fig. 6 through Fig. 9. Corresponding simulation parameters are listed in Table 2. Up to a moderate number of antennas, i.e., 32, can be activated in 5G NR in practical operating frequencies [61]. Therefore, we employ the number of MIMO antennas from 2 to 32 in Fig. 6 through Fig. 9 for simulation purpose. The SER and capacity of RSM-MRT with BPSK is compared to TSSK-MRC in Fig. 6 for $P = 4$ and $M = 2$ with Eve's SNR equal to 2 dB. As we expected RSM-MRT shows a superior performance to TSSK-MRC in Fig. 6(a). Hence, the system capacity of RSM-MRT displays a better performance than TSSK-MRC. The channel capacity is plotted with a solid line, and the secrecy capacity with a circle. Due to the independent channel matrices of Bob and Eve, the secrecy capacity of RSM-MRT achieves an isolated capacity. With TSSK-MRC, Bob's secrecy capacity is positive only when Bob's channel condition is superior to

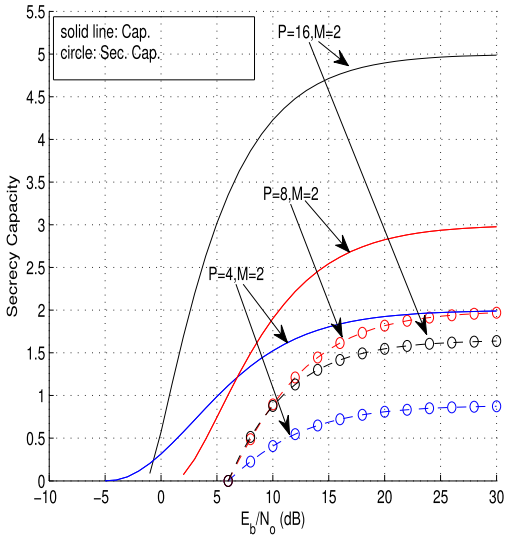


(a) SER

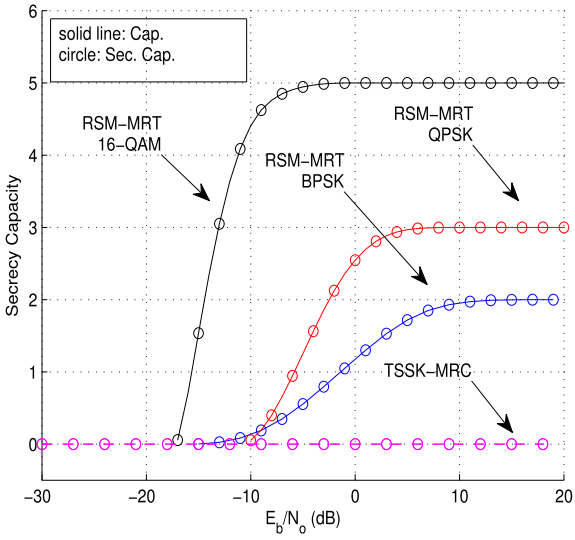


(b) Secrecy Capacity

FIGURE 8. TSSK-MRC, Eve SNR = 5 dB; RSM-MRT with 16-QAM; $P = 32, M = 2$.



(a) TSSK-MRC, Eve SNR = 6 dB



(b) RSM-MRT, Eve SNR = -20 dB, ..., 20 dB

FIGURE 9. Secrecy Capacity; TSSK-MRC, Eve SNR = 6 dB; RSM-MRT with BPSK ($P = 4, M = 2$), QPSK ($P = 8, M = 2$) and 16-QAM ($P = 32, M = 2$).

Eve's channel condition [62]. In Fig. 6(b), Bob can have a positive secrecy capacity when the SNR is greater than 2 dB since the SNR of Eve is 2 dB, i.e., the bit energy-to-noise ratio $E_b/N_o = 2$ dB. Both RSM-MRT and TSSK-MRC asymptotically approach 2 bits per second (bps) as the SNR increases as we expected. The asymptotic value of the secrecy capacity is only 1.27 bps with TSSK-MRC. However, RSM-MRT achieves an asymptotically isolated secrecy capacity of 2 bps. In Fig. 7, we can observe a similar result for RSM-MRT with quadrature phase-shift keying (QPSK) for $P = 8$ and $M = 2$ with Eve's SNR equal to 6 dB. The SER of RSM-MRT is superior to TSSK-MRC and the gap is larger than the case of BPSK due to an increased number of transmit antennas. With TSSK-MRC, Bob can experience a positive secrecy capacity only for E_b/N_o larger than 6 dB, since the SNR of Eve is 6 dB. On the other hand, RSM-MRT exhibits an isolated secrecy capacity independent of Eve's SNR. The capacity of both RSM-MRT and TSSK-MRC asymptotically approach 3 bps as the SNR increases. However, Eve's capacity displays 1.0 bps at E_b/N_o equal to 6 dB. Hence, Alice can transmit only 2 bps of secrecy data to Bob at a high SNR. We can also observe that Bob's secrecy capacity vanishes at an E_b/N_o below 6 dB with TSSK-MRC. With RSM-MRT, Alice can transmit a secrecy capacity equal to Bob's channel capacity at all SNR achieving 3 bps at a high SNR. The performance of 16-ary quadrature amplitude modulation (QAM) is shown in Fig. 8 with $P = 32$ and $M = 2$ with Eve's SNR equal to 5 dB. The SER and capacity of RSM-MRT is much better than TSSK-MRC, and the difference between the two systems is significantly larger than the difference between the two in BPSK or QPSK. The SNR of Eve is assumed to be 5 dB, and Bob can have secrecy capacity only when his SNR is

greater than 5 dB with TSSK-MRC. On the other hand, Bob can have an isolated secrecy capacity equal to his channel capacity when RSM-MRT with 16-QAM employed. With TSSK-MRC, Alice can transmit only 1.98 bps of secrecy data to Bob at a high SNR which is significantly reduced from his asymptotic channel capacity of 5 bps. With RSM-MRT, Bob can achieve a 5 bps secrecy capacity at a high SNR. Fig. 9 shows the performance of TSSK-MRC and RSM-MRT. The SNR of Eve is 6 dB in Fig. 9(a). All modulation schemes display a positive secrecy capacity for E_b/N_o greater than 6 dB with TSSK-MRC. In other words, Bob needs to have a better channel condition than Eve to communicate the secrecy data with Alice. It is observed that the secrecy capacity of Bob is significantly reduced from his channel capacity when 16-QAM modulation is employed. This is because the capacity of Eve is high at 6 dB SNR. The SNR of Eve is assumed to be the same as Bob's SNR varying -20 dB to 20 dB, in Fig. 9(b). RMS-MRT always maintains the isolated secrecy capacity that is equal to the channel capacity of Bob, independent of the channel condition of Eve. However, the secrecy capacity vanishes for all SNR with TSSK-MRC.

V. CONCLUSION

Cellular V2X can be implemented with 5G NR V2N with its reduced latency and enhanced reliability. We proposed 5G cellular DL V2X implementation using V2N with spatial modulation such as TSSK-MRC and RSM-MRT for groupcasting and unitcasting, respectively, in platooning and with extended sensors. Different types of communication are considered in NR-V2X to fulfill the requirements of many use cases of V2V, V2I, V2P, and V2N. The 5G NR V2N communication can be considered for improved road safety, increased traffic efficiency, and even infotainment. PLS provides security without any form of encryption in the upper layers, and is based on relatively simple signal processing technique. It is an excellent alternative to the computationally intensive and complicated cryptographic algorithms and techniques. Therefore, PLS can reduce the processing time and computational complexity, and satisfy the strong wireless channel security requirement. The main characteristics of the PLS are the noise and fading of the wireless channel, which are generally considered as impairments. However, they can be exploited to successfully hide messages. We proposed keyless PLS of 5G NR cellular DL V2N exploiting wireless channel fading characteristics.

We investigated the secrecy capacity of DL cellular systems. With TSSK-MRC, the secrecy capacity vanishes unless the legitimate receiver's channel characteristics are superior to those of the eavesdropper. If Bob's channel gain or SNR is better than Eve's, Bob can communicate with Alice with a certain secrecy capacity rate. Therefore, TSSK-MRC is suitable for NR C-V2N groupcast since every member in the group share the same traffic information. On the other hand, RSM-MRT employs the MRT based on the legitimate receiver's channel characteristics. Hence, only the legitimate receiver can detect the transmitted signal. However, the eavesdropper's channel is independent of the MRT channel if the eavesdropper is located a certain distance away from the legitimate receiver, which is very plausible in 5G mmWave communications. Therefore, despite the channel quality of the legitimate receiver and the eavesdropper, the legitimate receiver can always enjoy the secrecy capacity, which is the same as his isolated single channel capacity. Therefore, with RSM-MRT, NR C-V2N unicast can enjoy the complete secrecy capacity.

REFERENCES

[1] O. Al-Saadeh, G. Wikstrom, J. Sachs, I. Thibault, and D. Lister, "End-to-end latency and reliability performance of 5G in London," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.
[2] M. Muhammad and G. A. Safdar, "5G-based V2V broadcast communications: A security perspective," *Array*, vol. 11, pp. 1–13, Sep. 2021.
[3] M. Harounabadi, D. M. Soleymani, S. Bhadauria, M. Leyh, and E. Roth-Mandutz, "V2X in 3GPP standardization: NR sidelink in release-16 and beyond," *IEEE Commun. Standards Mag.*, vol. 5, no. 1, pp. 12–21, Mar. 2021.
[4] *NR; Physical Channels and Modulation*, document 3GPP TS 38.211, Version 16.3.0, Release 16, 2020.
[5] *Service Requirements for Enhanced V2X Scenarios*, document 3GPP TS 22.186, Version 16.2.0, Release 16, 2019.
[6] D. Zhao, H. Qin, B. Song, Y. Zhang, X. Du, and M. Guizani, "A reinforcement learning method for joint mode selection and power adaptation in the V2V communication network in 5G," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 2, pp. 452–463, Jun. 2020.
[7] R. Mesleh, "Spatial modulation: A spatial multiplexing technique for efficient wireless data transmission," Ph.D. dissertation, Dept. Elect. Comput. Eng., Jacobs Univ., Bremen, Germany, Jun. 2007.
[8] R. Mesleh, H. Haas, S. Sinanović, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2228–2241, Jul. 2008.
[9] T. Fath, M. Di Renzo, and H. Haas, "On the performance of space shift keying for optical wireless communications," in *Proc. IEEE Globecom Workshops*, Dec. 2010, pp. 990–994.
[10] M. Di Renzo, D. D. Leonardis, F. Graziosi, and H. Haas, "Space shift keying (SSK) MIMO with practical channel estimates," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 998–1012, Apr. 2012.
[11] M. Di Renzo and H. Haas, "A general framework for performance analysis of space shift keying (SSK) modulation for MISO correlated Nakagami-m fading channels," *IEEE Trans. Commun.*, vol. 58, no. 9, pp. 2590–2603, Sep. 2010.
[12] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Generalized space shift keying modulation for MIMO channels," in *Proc. IEEE 19th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2008, pp. 1–5.
[13] J. Fu, C. Hou, W. Xiang, L. Yan, and Y. Hou, "Generalised spatial modulation with multiple active transmit antennas," in *Proc. IEEE Globecom Workshops*, Dec. 2010, pp. 839–844.
[14] M. Di Renzo, H. Haas, and P. M. Grant, "Spatial modulation for multiple-antenna wireless systems: A survey," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 182–191, Dec. 2011.
[15] A. Younis, N. Serafimovski, R. Mesleh, and H. Haas, "Generalized spatial modulation," *Proc. Asilomar Conf. Signals, Syst., Comput.*, pp. 1498–1502, 2010.
[16] S. Sugiura, "Dispersion matrix optimization for space-time shift keying," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1152–1155, Nov. 2011.
[17] W. O. Popoola, E. Poves, and H. Haas, "Error performance of generalized space shift keying for indoor visible light communications," *IEEE Trans. Commun.*, vol. 61, no. 5, pp. 1968–1976, May 2013.
[18] R. Mesleh, R. Mehmood, H. Elgala, and H. Haas, "Indoor MIMO optical wireless communication using spatial modulation," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–5.
[19] R. Mesleh, H. Elgala, and H. Haas, "Optical spatial modulation," *J. Opt. Commun. Netw.*, vol. 3, no. 3, pp. 234–244, Mar. 2011.
[20] M. Maleki, K. Mohamed-Pour, and M. Soltanalian, "Receive spatial modulation in correlated massive MIMO with partial CSI," *IEEE Trans. Signal Process.*, vol. 67, no. 5, pp. 1237–1250, Mar. 2019.

[21] O. Hiari and R. Mesleh, "Hardware design and analysis for generalized receive space modulation techniques," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1616–1620, Sep. 2019.
[22] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.
[23] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.
[24] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Sep. 1949.
[25] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Aug. 1975.
[26] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[27] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, May 1978.
[28] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[29] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[30] Y. Liang, H. V. Poor, and S. S. Shitz, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
[31] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, Jul. 2008, pp. 524–528.
[32] A. Khisti and G. W. Wornell, "The MIMOME channel," in *Proc. 45th Annu. Allerton Conf.*, Monticello, IL, USA, Sep. 2007, pp. 625–632.
[33] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.
[34] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, Mar. 2011.
[35] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214–225, Jan. 2016.
[36] Z. Li, R. Yates, and W. Trappe, "Secret communication via multi-antenna transmission," in *Proc. 41st Ann. Conf. Inf. Sci. Syst.*, Mar. 2007, pp. 905–910.
[37] R. Bustin, R. Liu, H. V. Poor, and S. S. Shitz, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, pp. 1–8, Dec. 2009, doi: 10.1155/2009/370970.
[38] X. Xiaoqin and M. Gang, "Secrecy information transmission optimization of MIMO system," in *Proc. Cross Strait Quad-Regional Radio Sci. Wireless Technol. Conf. (CSQRWC)*, Taiyuan, China, Jul. 2019, pp. 1–3.
[39] L. Dong, S. Loyka, and Y. Li, "The secrecy capacity of Gaussian MIMO wiretap channels under interference constraints," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 704–722, Apr. 2018.
[40] H. Niu, B. Zhang, D. Guo, and Z. Bing, "Secrecy rate maximization for MIMO wiretap channels with a cooperative jammer using alternating optimization," in *Proc. 1st Int. Conf. Electron. Instrum. Inf. Syst. (EIIS)*, Jun. 2017, pp. 1–4.
[41] A. Umer, "Stochastic modeling and performance analysis of multi-tier HetNets," M.S. thesis, School Electr. Eng. Comput. Sci., Nat. Univ. Sci. Technol., Islamabad, Pakistan, 2017.
[42] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.
[43] J. Zhang, X. Ge, Q. Li, M. Guizani, and Y. Zhang, "5G millimeter-wave antenna array: Design and challenges," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 106–112, Apr. 2017.
[44] A. Umer, S. A. Hassan, H. Pervaiz, L. Musavian, Q. Ni, and M. A. Imran, "Secrecy spectrum and energy efficiency analysis in massive MIMO-enabled multi-tier hybrid HetNets," *IEEE Trans. Green Commun. Netw.*, vol. 4, no. 1, pp. 246–262, Mar. 2020.
[45] J. Ye, X. Ge, G. Mao, and Y. Zhong, "5G ultradense networks with nonuniform distributed users," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2660–2670, Mar. 2018.
[46] W. Wang, K. C. Teh, S. Luo, and K. H. Li, "Physical layer security in heterogeneous networks with pilot attack: A stochastic geometry approach," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6437–6449, Dec. 2018.
[47] S. Kusaladharma, W.-P. Zhu, and W. Ajib, "Stochastic geometry-based modeling and analysis of massive MIMO-enabled millimeter wave cellular networks," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 288–301, Jan. 2019.
[48] M. Maleki, H. R. Bahrami, and A. Alizadeh, "On MRC-based detection of spatial modulation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3019–3029, Apr. 2016.
[49] M. K. Simin and M. Alouini, *Digital Communication over Fading Channels*. Hoboken, NJ, USA: Wiley, 2004.
[50] B. M. ElHalawany, A. A. A. El-Banna, and K. Wu, "Physical-layer security and privacy for vehicle-to-everyting," *Commun. Mag.*, vol. 57, no. 10, pp. 84–90, Oct. 2019.
[51] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, 1st Quart., 2020.
[52] A. Sanenga, G. Mapunda, T. Jacob, L. Marata, B. Basutli, and J. Chuma, "An overview of key technologies in physical layer security," *Entropy*, vol. 22, no. 11, p. 1261, Nov. 2020.
[53] M. Campagna, L. Chen, Ö. Dagdelen, J. Ding, J. K. Fernick, N. Gisin, D. Hayford, T. Jennewein, N. Lütkenhaus, M. Mosca, B. Neill, M. Pecen, R. Perlner, G. Ribordy, J. M. Schanck, D. Stebila, N. Walenta, W. Whyte, and D. Z. Zhang, "Quantum safe cryptography and security: An introduction, benefits, enablers and challenges," Eur. Telecommun. Standards Inst., Sophia Antipolis, France, ETSI White Paper 8, Jun. 2015.
[54] L. Wang, *Physical Layer Security in Wireless Cooperative Networks* (Wireless Networks). Cham, Switzerland: Springer, 2018.
[55] J. M. Hamamreh, H. M. 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. 1773–1827, 2nd Quart., 2019.
[56] D. Gesbert, H. Bolcskei, D. A. Gore, and A. J. Paulraj, "Multiple-input-multiple-output measurements and modeling in Manhattan," *IEEE Trans. Commun.*, vol. 50, no. 12, pp. 1926–1934, Dec. 2002.
[57] R. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: Wiley, 1968.
[58] S. X. Ng and L. Hanzo, "On the MIMO channel capacity of multidimensional signal sets," *IEEE Trans. Veh. Technol.*, vol. 55, no. 2, pp. 528–536, Mar. 2006.
[59] S. R. Aghdam, T. M. Duman, and M. Di Renzo, "On secrecy rate analysis of spatial modulation and space shift keying," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, Constanta, Romania, May 2015, pp. 63–67.
[60] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley, 1991.
[61] F. Rinaldi, A. Raschellà, and S. Pizzi, "5G NR system design: A concise survey of key features and capabilities," *Wireless Netw.*, vol. 27, no. 8, pp. 5173–5188, Oct. 2021.
[62] S. Sinanovic, N. Serafimovski, M. Di Renzo, and H. Haas, "Secrecy capacity of space keying with two antennas," in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, Sep. 2012, pp. 1–5.