Split Antenna Array in Millimeter Wave for Secure Vehicular Communication

Shah Marjan[1,*], *Lin* Bai[1] , and *Chao* Han[1]

[1] School of Electronics and Information Engineering, Beihang University Beijing, China

Abstract. The small carrier wavelength at millimeter wave (mm-wave) frequencies features a large number of co-located antennas. Wireless networks with directional antennas using beamforming at mm-wave also have potential to provide an enhanced security in the vehicular communication system. Large bandwidth of mm-wave can provide auto drive and safety linked functionalities, However, safety and efficiency of the vehicular transportation system can be jeopardized by many kinds of attacks by eavesdroppers, physical layer security can work as an extra layer of security for wireless communication systems. To secure communication in-between Vehicles, an Analog precoding based physical Layer technique for mm-wave vehicular communication systems is presented in the paper. The proposed technique works by exploiting large Antenna arrays at millimeter waves and provide a secure directional transmission with low power consuming phase shifters and single Radio Frequency Chain. Larger antennas arrays are split into two subsets, one for transmission of data and another for generating noise. The proposed technique offers improved coherent transmission at the legitimate receiver and by introducing artificial noise to the eavesdroppers at random directions. This outcome in low SNR for the eavesdroppers, hence hacking information becomes extremely difficult. Numerical and Simulation results show the superior performance of the proposed technique compared to traditional physical layer security technique and conventional array technique.

1 Introduction

Millimeter wave (mm-wave) requires a huge number of antennas working synchronously for its propagation, which can play an important role in the vehicular communication systems. Millimeter wave's usage in vehicular communication technologies will provide applications for driver assistance, traffic efficiency, and safety[1,2]. A communication system in general face security threats, whereas vehicular communication systems faces security threats with a human life at stake. These threats can be dangerous for the safety of the drivers, people around, infrastructures and vehicles, also it can make the efficiency of the vehicular transportation system vulnerable. Typical threads include message falsification [2], spoofing [3], message relay [4], eavesdropping [5], and many others [2-5].

Many digital signature based encryption protocols which belong to higher layers are proposed in [6,7]. But these encryption protocols worked for lower frequency vehicular communication systems. The rapid change from low frequencies to high frequencies is required as a need of bandwidth, which erupted new challenges for the old encryption techniques. These key based encryption technique regular exchange keys, hence degrade system by extra communication overhead [1,2]. Key distribution in lower frequencies is done by broadcasting the key, which gives the edge to the old encryption techniques. Communication in mm-wave uses beamforming, which is an important part of mm-wave communication, hence sharing keys using beamforming would not be an easy task. This makes the traditional security techniques having high latencies for vehicular communication using mm-wave, which is a bottleneck for the safety related Vehicular systems. Time sensitive application, decentralization and huge size increase (2+ billion by [8]) of Vehicular networks make conventional security techniques complex and engulfing high latencies, which give space to new vehicular communication security techniques.

Increased complexities of traditional security techniques in mm-wave, give space for physical layered security techniques [9-18], which uses lowest layer to provide secure vehicular communication links. These physical layer techniques use Antenna subset array [9], digital beamforming [14,19,20], distributed array [13,14], and recent most switched array [15,17,18].

Digital beamforming calibrates antenna weights, which circulates noise is all other directions other than the receiver. In digital precoding there are hardware and power constraints in mm-wave systems [21], hence making digital precoding not realistic with a huge number of transmitting antennas at mm-wave. In distributed array technique [13,14], relays are used in communication that provides noise to the eavesdroppers and data at the receiver. Switched array technique [15,17,18] and antenna subset array [9] used multiple subsets of antennas to transmit

*Corresponding author: shahmarjan@buaa.edu.cn

every symbol, which results in coherent time and noise in all other directions where eavesdroppers can be present. Switched array technique efficiently randomizes the amplitude and phase of the received symbol for any eavesdropper present along the side lobes. But recently this technique was exploited by performing sparsity in the transmit antenna array and hence able to detectsymbols with the help of this attack [22]. Conventional array uses all antennas to transmit, hence no physical layer security is provided to the communication systems. In this paper we proposed a new security technique based on physical layer for vehicular communication systems that provides keyless communication security, it does not require fully digital precoding architecture [14,19,20]. We assumed single transmitter, a single receiver and two eavesdroppers at different positions. We used analog precoding with random antenna selection for the receiver to receive the transmitted symbol and for eavesdroppers to receive noise by randomizing radiations on the side lobes. This provides incoherent transmission at the legitimate receiver and high value of noise at the eavesdroppers received signals. This proposed technique is also immune to the attack mentioned in [22], because random sets of antennas are used for transmission of each symbol.

2 System Model

We consider a mm-wave vehicular communication system with a Vehicle (V_T) as a transmitter and a vehicle (V_R) as a receiver in the existence of two eavesdroppers at different angles and distance from the (V_T) shown below in figure 1.

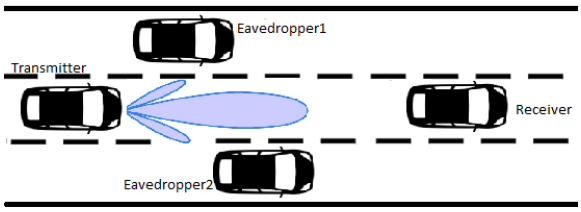

Fig. 1. Eavesdropper and Legitimate Receiver positions

The V_T is consists of N_T antennas and a RF chain which is shown in figure 2, this makes it an analog beamforming architecture. Whereas V_R consists of N_R antennas. The two eavesdroppers as shown in figure 1 are equipped with N_E antennas each.

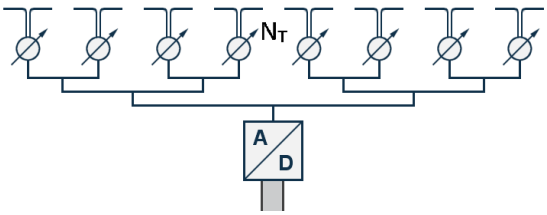

Fig. 2. Analog Array Architecture

We consider uniform linear array (ULA) which has isotropic antennas, the same approach can be applied to multidimensional arrays on a rectangular and circular grid. we posit an N_T elements linear array with antennas uniformly placed along the x-axis and with the array centered at the origin. Since the uniform linear array in this scenario is positioned on the x-y plane cannot resolve elevation (ϕ), the receiver's angular location is solely specified by azimuth angle (θ). we assume that legitimate receiver's location has been acquired using beam training, where as it is unaware about the location of the two eavesdroppers in the scenario.

The transmit data symbol by the transmitter is s(k) ϵ C, where k is the transmitted index of the symbol and E[|s(k)|] = 1. $f_n = [f_1, f_2, \dots, f_{N_T}]$ is the transmit beamforming vector denoted by f_n having complex weight at the transmit antenna array n. whereas at the receiver, a combined receiver is used on all of the received signals, with a combining vector $w = [w_1, w_2, \dots, w_{N_R}]^T$, Where N_R is the total number of antennas which are mounted on the transceiver of the V_T. Invoking a narrow band channel model at mm-wave, because in mm-wave the line of sight (LOS) component is usually the dominate path. And a perfect synchronization and symbol rate among the transmitter and the receiver is assumed.

The signal received can be equated as $y(k,\theta) = h^*(\theta)\ f\ s(k) + \ v(k)$. By placing power and path loss components we get.

$$\mathbf{y}(\mathbf{k}, \boldsymbol{\theta}_{E|R}) = \sqrt{\boldsymbol{P}\boldsymbol{\alpha}_{E|R}}\ \ \mathbf{h}^*(\boldsymbol{\theta}_{E|R})\ \mathbf{f}\ \ \mathbf{s}(\mathbf{k}) + \ \mathbf{v}(\mathbf{k}) \quad (1)$$

Here k is the index of the data symbol to be received and θ is the Azimuth angle of departure (AoD) from the transmit antenna array, $\alpha_{E|R}$ shows the path loss component of the communication, P is the transmitted symbol power provided. H is the channel matrix of $N_R * N_T$ that shows the mm-wave channel. $h^*_{E|R} = w^* H(\theta_{E|R}, \phi)$ is the channel after combination of the receiver and $v(k) \sim CN(0, \sigma^2)$ is assumed to be the noise added while transmission occurs. So channel is given by.

$$H(\theta_{E|R}, \phi) = g\ \ a_t^*(\theta)\ a_r(\phi) \quad (2)$$

$a_t(\theta)$ and $a_r(\phi)$are vectors which represents the receiver and transmit array response as shown.

$$a_t(\theta) = \exp(\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2}\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta), \exp(\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2}\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta), \dots, \exp(-\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2}\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta) \quad (3)$$

$$a_r(\phi) = \exp(\mathrm{j}\left(\frac{\mathrm{N_R}-1}{2}\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\phi), \exp(\mathrm{j}\left(\frac{\mathrm{N_R}-1}{2}\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\phi), \dots, \exp(-\mathrm{j}\left(\frac{\mathrm{N_R}-1}{2}\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\phi) \quad (4)$$

And g is a random variable to consider the small scale fading caused by Doppler spread and multipath. For frequencies below 6Ghz, the g is distributed as Gaussian random variable[23]. Whereas for 60Ghz the value of g is still not known, but a good beamforming at the transmitter

provides the communication with a small Doppler spread and as a result give larger coherence time [24]. So by considering the value of g=1, we supposed a single LOS between transmitter and receiver. We also assume $w = a_r(\phi)$ means beam is aligned towards the receiver V_R. Received signal becomes as shown in (1), where N_R is the gain at the receiver array. ULA with a spacing between antennas $d \leq \frac{\lambda}{2}$ is taken into assumption to avoid creating grating lobes. $h^*(\theta) = \sqrt{N_R}\, g\, a^*(\theta)$ Shows the channel.

$$\begin{aligned} &\mathrm{h}^*(\theta) \\ &= \sqrt{N_R}\ \mathrm{g}\ [\ \exp(-\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2}\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta), \\ &\qquad \exp(-\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2}\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta), \\ &\qquad \ldots, \exp(\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2}\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta)] \end{aligned} \tag{5}$$

Here $h^*(\theta)$ is the channel for the communication link.

3 Analog Bream Forming

In this section of the paper, we introduce a physical layered security technique based on Analog beamforming. This technique randomizes the information symbols at potential eavesdroppers using phase shifters and no need for multiple RF chains and antenna switches as shown in figure 2, hence categorized as analog based design. The conventional architecture uses all antennas to transmit symbols to the receiver [18], Proposed technique split antenna array into 2 subsets, one for sending a symbol to the receiver and second for generating noise in an unwanted direction towards the eavesdroppers. This way the eavesdroppers will receive noise like signals, whereas the receiver will only observe a reduction in gain.

Let $A_M(k)$ be the subset randomly selected from N_T with M antennas, where $m \epsilon A_m(k)$ and $A_N(k)$ is the subset containing the remaining antennas from N_T with $N_T - M$ antennas, where $n \epsilon A_n(k)$ from ULA.

$$\varphi(k) = \begin{cases} \left(\frac{\mathrm{N_T}-1}{2} - m\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta_R) & if\ m > \frac{N_T}{2} \\ \left(\frac{\mathrm{N_T}-1}{2} - n\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta_R) + \pi & if\ n < \frac{N_T}{2} \end{cases} \tag{6}$$

Whereas the beam forming vector $f(k) = \frac{1}{\sqrt{N_T}} e^{j\varphi(k)}$, and the angle θ_R is the V_R direction at the tramit antenna array. Then

$$f_m(k) = \frac{1}{\sqrt{N_T}}\left[\exp\left(\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2} - m\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta_R)\right)\right] \tag{7}$$

$$f_n(k) = \frac{1}{\sqrt{N_T}}\left[\exp\left(\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2} - n\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta_R) + \pi\right)\right]$$

$$f_n(k) = -\frac{1}{\sqrt{N_T}}\left[\exp\left(\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2} - n\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta_R)\right)\right] \tag{8}$$

Using Eq. (3), (5), (7) and (8) and putting values in (1), the received signal at the receiver and eavesdropper becomes.

$$\begin{aligned} y(k,\theta_{E|R}) = &\sqrt{\frac{N_{E|R}\, P\alpha_{E|R}}{N_T}}\, g\ s(k)\,. \\ &\Sigma_{\mathrm{m}\epsilon\mathrm{A_m}} exp\left(-j\left(\left(\frac{N_T-1}{2}\right) m\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta_R)\right). \\ &exp\left(j\left(\left(\frac{N_T-1}{2}\right)m\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta)\right) - \\ &\Sigma_{\mathrm{n}\epsilon\mathrm{A_n}} exp\left(-j\left(\left(\frac{N_T-1}{2}\right) - n\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta_R)\right). \\ &exp\left(j\left(\left(\frac{N_T-1}{2}\right) - n\right)\left(\frac{2\pi d}{\lambda}\right)\cos(\theta)\right) \end{aligned} \tag{9}$$

$$y(k,\theta_{E|R}) = \sqrt{p\alpha}\, g\, \sqrt{N_{E|R}}\ \beta\ \ s(k)\ +\ v(k) \tag{10}$$

Received signal = Effective Channel Gain x Array Gain x Information Symbol x Additive Noise

$$\beta = \sqrt{\frac{1}{N_T}}\left[\Sigma_{\mathrm{m}\epsilon\mathrm{A_m}(k)}\ \exp\left(\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2} - m\right)\left(\frac{2\pi d}{\lambda}\right)a\right) - \Sigma_{\mathrm{n}\epsilon\mathrm{A_n}(k)}\ \exp\left(\mathrm{j}\left(\frac{\mathrm{N_T}-1}{2} - n\right)\left(\frac{2\pi d}{\lambda}\right)a\right)\right] \tag{11}$$

where value of $a = (\cos(\theta) - cos(\theta_R))$. When eavesdropper1 (E_1) or eavesdropper2 (E_2) are aligned in direction of legitimate receiver, hence $\theta = \theta_R$, the antenna gain becomes $\beta = \frac{2M-N_T}{\sqrt{N_T}}$ which is a constant value. Whereas when $\theta \neq \theta_R$, β reshapes into a complex Gaussian random variable, hence this randomize the antenna array gain in the random directions, and which in result performs the function of jamming in the direction of the eavesdroppers. In the proposed technique we suppose large value of N_T, hence value of β converges into a Complex Gaussian Variable, having Mean value of,

$$\mathrm{E}[\beta] = \frac{(2M-N_T)}{N_T\sqrt{N_T}} \cdot \frac{\sin\left(\frac{N_T \pi d}{\lambda} a\right)}{\sin\left(\frac{\pi d}{\lambda} a\right)} \tag{12}$$

And Variance value of,

$$Var[\beta] = \frac{4MN_T - 4M^2}{N_T^2} \tag{13}$$

Omitted proof because of the limitation of space.

4 Split antenna array secrecy

We measure the proposed physical layer technique performance on the basis of secrecy in this section. The

transmitter is assumed to have knowledge of the target V_R but lacks that of the $E_1 and\ E_2$. Secrecy capacity of the Gaussian wiretap channel is denoted by C_S is the difference between the capacity of the main and the wiretap channels. By using this definition and denoting the legitimate receiver and eavesdropper by C_R and C_E respectively.

$$C_S = \begin{cases} C_R - C_E & if\ C_R > C_E \\ 0 & otherwise \end{cases} \quad (14)$$

The secrecy rate R is shown in bits per second per hertz used and can be calculated by

$$R = \left[\log_2(1+\gamma_R) - \log_2\left(1+\gamma_{E_n}\right)\right]^+ \quad (15)$$

Where γ_R is the SNR at the legitimate V_R, γ_{E_n} is the SNR at the eavesdroppers at different direction as well as distance and a^+ denotes $\max(0,a)$ a maximum function. Using Eq. (10) the value of SNR at the legitimate receiver, when the angle $\theta = \theta_R$ is expressed as.

$$\gamma_R = \frac{P\alpha_R N_R g_R^2 (2M - N_T)^2}{N_T\,\sigma^2} \quad (16)$$

The SNR at the eavesdropper can be expressed as,

$$\gamma_E = \frac{P\alpha_E N_E g_E^2 \mathrm{E}[\beta^2]}{P\alpha_E N_E g_E^2 Var[\beta] + \sigma_E^2} \quad (17)$$

Here N_E is the number of antennas at different eavesdroppers, g_E is the channel gain at the eavesdroppers, α_E is the path loss at the eavesdropper and noise $Z_E(k) \sim CN(0,\sigma_E^2)$. To derive SNR at the eavesdropper we suppose the larger value of N_T, hence the term β can be dissolved almost by the values of its mean and variance. Putting the value into the Eq. (17) from Eq. (12)(13).

$$\gamma_E = \frac{P\alpha_E N_E g_E^2 (2\mathrm{M}-\mathrm{N_T})^2}{N_T P\alpha_E N_E g_E^2 (4MN_T - 4M^2) + N_T^3 \sigma_E^2} \cdot \frac{\sin\left(\frac{N_T \pi d}{\lambda} a\right)}{\sin\left(\frac{\pi d}{\lambda} a\right)} \quad (18)$$

Using equation (16) and (18), we can calculate secrecy rate R of equation (15).

$$R = \left[\log_2\left(1 + \frac{P\alpha_R N_R g_R^2 (2M-N_T)^2}{N_{T\sigma^2}}\right) - \log_2\left(1 + \frac{P\alpha_E N_E g_E^2 (2\mathrm{M}-\mathrm{N_T})^2}{N_T P\alpha_E N_E g_E^2 (4MN_T - 4M^2) + N_T^3 \sigma_E^2} \cdot \frac{\sin\left(\frac{N_T \pi d}{\lambda} a\right)}{\sin\left(\frac{\pi d}{\lambda} a\right)}\right)\right]^+ \quad (19)$$

5 Numerical and simulation results

In this section, the proposed physical layer security technique is used to check performance in the presence of eavesdroppers at different angles and distances from the transmitter using vehicle to vehicle communication. E_1 is present at an angle of 95 degrees and E_2 is present at an angle of 85 degrees. The system is operated at a 60Ghz frequency, with 50Mhz bandwidth and an average power of 37dBm is provided. The value of g is taken a constant 1 because at the 60Ghz value of g is unknown. Path loss exponent is set to 2 and distance from the transmitter to receiver is 30meters whereas the distance from the V_T to E_1 is 5 meter and E_2 is 10 meter. The number of antennas at both the eavesdroppers are $N_{E1} = N_{E2} = 512$, and the antennas set at the V_R is $N_R = 16$. The value of N_T has been set 32 and 64 antennas.

In figure 3 we show secrecy rate against the angular location of the proposed security technique, while setting the value of $N_T = 32$ transmit antennas, whereas E_1 is evaluated in 3(a) and E_2 in 3(b). In this case of N_T, we observed high secrecy rate at all angular locations other than

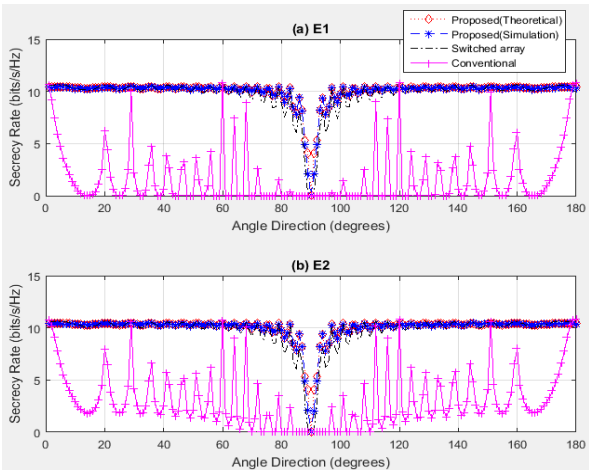

Fig. 1. Secrecy Rate vs. Angular Direction When steered at $\theta_R = 90^o$, $N_T = 32$ and $M = 30$, whereas E_1 is at a distance of 5 meter and 95° and E_2 is at a distance of 10 meter and 85°.

the angular location of the receiver $\theta_R = 90^o$. we also observed the switched array technique, and conventional array technique [18-21]. Switched array technique have better results compared to the conventional array technique, the reason is that conventional array provide a stable and constant radiation pattern at the output of the antenna array, whereas switched array randomizes the pattern, hence provide jamming the eavesdroppers. Proposed technique beats other two techniques by using all antennas, many for transmission and few for generating noise to achieve better performance. Both E_1 and E_2 observed low SNR. Effect of the distance of eavesdropper from the transmitting vehicle is observed in path loss .

In figure 4 we show secrecy rate against the angular location of the proposed security technique, while setting the value of $N_T = 64$ transmit antennas. This case of N_T also provided low SNR at both E_1 and E_2 as the case of 32 transmit antennas.

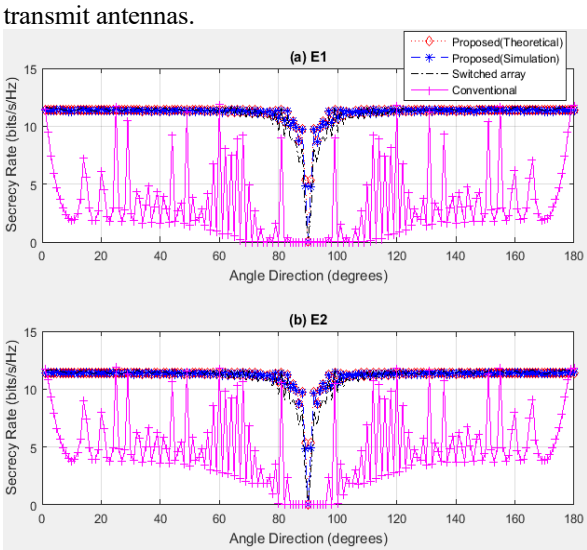

Fig. 4. Secrecy Rate vs. Angular Direction When steered at $\theta_R = 90^o$, $N_T = 64$ and $M = 60$, whereas E_1 is at a distance of 5 meter and 95° and E_2 is at a distance of 10 meter and 85°.

When E_1 and E_2 are placed at the same angle as the V_R, the secrecy is zero, but this should not be the case for LOS vehicular communication. The proposed technique make use of all antennas, therefore breaching is much more difficult and low SNR values are received at the eavesdroppers.

In some instances of figure 3(a), 3(b), 4(a) and 4(b) the conventional array technique shows peaks of better security when compared to switched array and proposed technique. This is observed because the eavesdropper position's at a null space created by transmitter array pattern. Since the conventional array technique makes use of all the antennas in the array for transmitting any data symbol, hence results in slightly higher secrecy when the eavesdropper is at the null space.

Finally figure 5 shows secrecy rate against the subset size (M) of the proposed security technique. Observation shows that our technique provides better secrecy when the

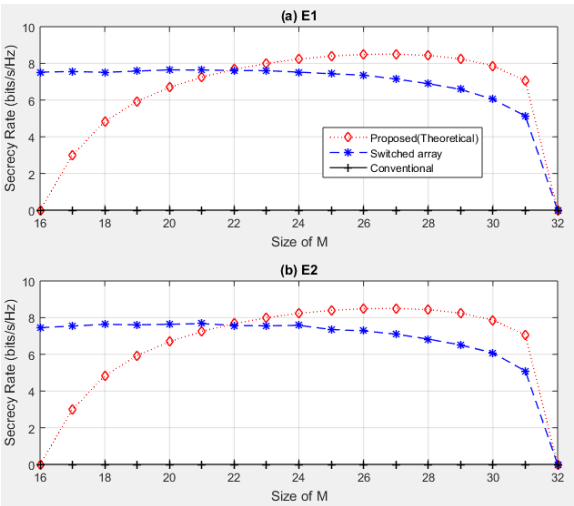

Fig. 5. Secrecy Rate vs. Subset Size M whereas $\theta_R = 90^o$ for both E_1 and E_2 and $N_T = 32$.

value of M is high, whereas switched array [15,17,18] and conventional both provides low secrecy at higher values of M as compared to proposed technique. Selecting the value of M in figure 5 from 16 to 32 shows that a large number of antennas are selected for transmitting the data and less number of antennas are used to create jamming towards unwanted direction. When the value of M equals 16, we receive Zero secrecy because both beams forming vectors are of the same size. Hence proposed technique performs better when the value of M is greater than 22 antennas for a total number of 32 antennas.

The proposed technique uses mm-waves, hence provides a larger number of the antenna array which provides space for sparing few antennas for security purpose. hence sacrificing antennas for physical layer security provides the proposed technique with the benefit of high secrecy rate.

6 Conclusion

In this paper, we proposed a simplified analog based physical layer security technique using mm-wave analog precoding for vehicular communication. The proposed technique makes use of the larger antenna array at the mm-wave frequencies to generate noise like signal by decrease the SNR at the eavesdroppers with sensitive receivers, whereas slight SNR decrease is felt at the target receiver. This enhances the security at the vehicle transmit and the vehicle receive. The proposed technique provides high secrecy rate unlike the conventional and switched array techniques. Lower frequencies use encryption/decryption keys to secure communication, whereas mm-waves beamforming need provides physical layer security without the extra burden at both transmitter and receiver. The proposed technique also provides a better use of a large number of antennas possible at mm-wave communication system. Thus the proposed security technique proves to be simple and easily applicable for road safety, time critical, driving assistance and other application in vehicular communications.

References

1. J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, et al., "*Vehicle-to-vehicle communications: Readiness of V2V technology for application*," (2014).
2. M. Raya, P. Papadimitratos, and J.-P. Hubaux, "*Securing vehicular communications," IEEE Wireless Communications*, **vol. 13**, (2006).
3. M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, et al., "*Security vulnerabilities of connected vehicle streams and their impact on cooperative driving*," IEEE Communications Magazine, **vol. 53**, pp. 126-132, 2015.
4. C. Laurendeau and M. Barbeau, "*Threats to Security in DSRC/WAVE*," in International Conference on Ad-Hoc Networks and Wireless, (2006), pp. 266-279.
5. A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, et al., "*Attacks on inter vehicle communication systems-an analysis*," Proc. WIT, pp. 189-194, (2006).
6. J.-P. Hubaux, S. Capkun, and J. Luo, "*The security and privacy of smart vehicles*," IEEE Security & Privacy, **vol. 2**, pp. 49-55, (2004).
7. J. Guo, J. P. Baugh, and S. Wang, "*A group signature based secure and privacy-preserving vehicular communication framework*," in 2007 Mobile Networking for Vehicular Environments, (2007), pp. 103-108.
8. D. Sperling and D. Gordon, *Two billion cars: driving toward sustainability*: Oxford University Press, (2009).
9. N. N. Alotaibi and K. A. Hamdi, "*A low-complexity antenna subset modulation for secure millimeter-wave communication*," in 2016 IEEE Wireless Communications and Networking Conference, (2016), pp. 1-6.
10. A. Khisti and G. W. Wornell, "*Secure transmission with multiple antennas I: The MISOME wiretap*

channel," IEEE Transactions on Information Theory, **vol. 56**, pp. 3088-3104, (2010).

11. M. P. Daly and J. T. Bernhard, "*Directional modulation and coding in arrays*," in Antennas and Propagation (APSURSI), 2011 IEEE International Symposium on, (2011), pp. 1984-1987.
12. Y. Ding and V. F. Fusco, "*Constraining directional modulation transmitter radiation patterns*," IET Microwaves, Antennas & Propagation, **vol. 8**, pp. 1408-1415, (2014).
13. S. Goel and R. Negi, "*Guaranteeing secrecy using artificial noise*," IEEE transactions on wireless communications, **vol. 7**, (2008).
14. J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "*Wireless secrecy regions with friendly jamming*," IEEE Transactions on Information Forensics and Security, **vol. 6**, pp. 256-266, (2011).
15. E. J. Baghdady, "*Directional signal modulation by means of switched spaced antennas*," in Military Communications Conference-Crisis Communications: The Promise and Reality, 1987. MILCOM 1987. IEEE, (1987), pp. 0938-0942.
16. M. P. Daly and J. T. Bernhard, "*Beamsteering in pattern reconfigurable arrays using directional modulation*," IEEE Transactions on Antennas and Propagation, **vol. 58**, pp. 2259-2265, (2010).
17. N. N. Alotaibi and K. A. Hamdi, "*Switched phased-array transmission architecture for secure millimeter-wave wireless communication*," IEEE Transactions on Communications, **vol. 64**, pp. 1303-1312, (2016).
18. N. Valliappan, A. Lozano, and R. W. Heath, "*Antenna subset modulation for secure millimeter-wave wireless communication*," IEEE Transactions on Communications, **vol. 61**, pp. 3231-3245, (2013).
19. S. Liu, Y. Hong, and E. Viterbo, "*Practical secrecy using artificial noise*," IEEE Communications Letters, **vol. 17**, pp. 1483-1486, (2013).
20. X. Zhang, X. Zhou, and M. R. McKay, "*Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks*," IEEE Transactions on Information Forensics and Security, **vol. 8**, pp. 1802-1814, (2013).
21. Z. Pi and F. Khan, "*An introduction to millimeter-wave mobile broadband system*s," IEEE communications magazine, **vol. 49**, (2011).
22. C. Rusu, N. González-Prelcic, and R. W. Heath, "*An attack on antenna subset modulation for millimeter wave communication*," in Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on, (2015), pp. 2914-2918.
23. M. Boban, J. Barros, and O. K. Tonguz, "*Geometry-based vehicle-to-vehicle channel modeling for large-scale simulation*," IEEE Transactions on Vehicular Technology, **vol. 63**, pp. 4146-4164, (2014).
24. V. Va, J. Choi, and R. W. Heath, "*The impact of beamwidth on temporal channel variation in vehicular channels and its implications*," IEEE Transactions on Vehicular Technology, **vol. 66**, pp. 5014-5029, (2017).