Beamforming for Secure Antenna Subset Modulation in Micro-wave Systems

Yonggu Lee*, Bumchul Sun*, Jingoog Kim†, Jinho Choi*
*School of Information and Communications,
Gwangju Institute of Science and Technology (GIST), Korea
†Agency for Defense Development (ADD), Korea
Email: *{yglee1096, sunbc, jchoi0114}@gist.ac.kr, †jingoog@add.re.kr

***Abstract*—For secure transmissions in millimeter (mm)-wave systems, antenna subset modulation (ASM) has been studied by exploiting a high directivity due to sparse-nature scattering environments. In this paper, we consider ASM for secure transmissions under rich scattering environments in micro-wave systems. Since no directivity can be exploited for secure transmissions, we use beamforming with ASM. In order to see the performance, we derive outage probabilities and show that an eavesdropper can have a high outage probability, while a legitimate receiver has a low outage probability. We also consider partial selection for ASM to improve the performance.**

***Index Terms*—Antenna subset modulation, beamforming, micro-wave system, outage probability.**

I. Introduction

Physical-layer security in wireless communications has been extensively studied [1], [2], as it can exploit random nature of wireless channels for secure communication with perfect secrecy [3]. With multiple antennas, the secrecy rate is analyzed in [4] and beamforming approaches are studied [5].

Among physical-layer security techniques, direction modulation (DM) technique was investigated to exploit the spatial selectivity using antenna arrays in [6], [7], [8]. In [6], [7], an approach that can form a beam by phase shifting of each antenna towards a target angle is proposed to ensure that an eavesdropper located in different angle is not able to receive any useful information. However, this approach needs a number of RF chains when the array has a number of antennas elements. In [8], a DM technique using a switched antenna array for secure communications was proposed with spreading sequence for low probability intercept (LPI). However, the length of spreading sequences has to be smaller than the number of antennas and if an eavesdropper knows the sequence, antenna switching cannot be secure.

In [9], [10], a physical-layer security scheme for distributed detection which uses channel state information (CSI) as an encryption key was presented in wireless sensor networks. The sensors are divided into non-flipping group, dormant group and flipping group according to sensor's CSI. This approach is similar to DM in terms of random bit flipping in RF stage that depends on (random) channel gains.

In [11], ASM is studied for secure transmissions in mm-wave systems. ASM can be seen as a low-complexity DM for secure transmissions. As in DM, ASM uses RF modulation and makes an eavesdropper confused using random antenna selection.

There exists an attack model for ASM in mm-wave systems [12]. If an eavesdropper can obtain multiple measurements at different angles simultaneously, it is possible to estimate secret symbols and the target angle.

In this paper, we consider ASM in micro-wave channels that might be more popular in wireless applications. In this case, we are not able to exploit directivity or directional beam. To apply ASM, we need to have the CSI for baseline beamforming together with power allocation. Furthermore, since the signal-to-noise ratio (SNR) becomes a random variable, we need to have a different performance metric, which is the outage probability in this paper. To improve the performance of ASM in micro-wave channels, we modify ASM and show that the performance can be improved in terms of outage probability. Note that the attack for ASM in [12] can be ineffective in micro-wave channels as random beamforming with power allocation can make the eavesdropper's SNR low.

Notation: Upper-case and lower-case boldface letters are used for matrices and vectors, respectively. $\mathbf{A}^{\mathrm{H}}$ denotes Hermitian transpose of $\mathbf{A}$. $\mathbf{A}^*$ denotes the conjugate of $\mathbf{A}$. The elementwise multiplication is denoted by $\odot$. The statistical expectation is denoted by $\mathbb{E}[\cdot]$. $\mathcal{CN}(m, \sigma^2)$ represents the distribution of circularly symmetric complex Gaussian (CSCG) random vector with mean m and variance σ^2.

II. System Model

Suppose that a legitimate transmitter (Alice) sends confidential data to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve). Alice is equipped with an array of L antenna elements for beamforming to transmit confidential data to Bob, and Bob and Eve have a single antenna. For ASM, Alice uses only $M(M < L)$ active antennas among L antennas in the array to send confidential data to Bob as in [11]. However, for ASM in this paper, we consider micro-wave channels which is different from [11] where ASM is studied for mm-wave channels.

A. Channel Models

Throughout the paper, we consider Rayleigh slow fading channels in time-division duplexing (TDD) manner. Thus, Alice can estimate the channel to Bob from a pilot signal

(or uplink training signal) transmitted by Bob. In addition, we assume that the coherence time is longer than the total time for uplink training and data transmission so that the estimated channel from uplink training can be used for beamforming. We denote the i-th channels from Alice to Bob and Eve by h_i and g_i, respectively. Thus, Bob's channel and Eve's channel are given by

$$\begin{aligned} h_i &= \alpha_i^h e^{j\theta_i^h} \\ g_i &= \alpha_i^g e^{j\theta_i^g}, \end{aligned} \tag{1}$$

where $h_i, g_i \sim \mathcal{CN}(0,1)$ for $i = 1, 2, ..., L$ and $\alpha_i^h, \alpha_i^g \in [0, \infty)$ and $\theta_i^h, \theta_i^g \in [-\pi, \pi)$ follow a Rayleigh distribution and a uniform distribution, respectively. Then, let $\mathbf{h}^{\mathrm{T}} = [h_1\ h_2\ ...\ h_L]$ and $\mathbf{g}^{\mathrm{T}} = [g_1\ g_2\ ...\ g_L]$ denote the channel vectors of size $1 \times L$ from Alice to Bob and Eve, respectively.

B. ASM

In this subsection, we explain ASM [11] for micro-wave systems. As ASM in mm-wave systems, there are M RF chains but the number of antennas is L at the transmitter. In addition, M active antennas are selected by RF switches randomly. While the channel coefficients have the same magnitude in mm-wave channels [11], they are different in micro-wave channels [4]. Thus, the power allocation can play a crucial role in ASM under micro-wave channel environments. In other words, it is necessary to control the transmit power in micro-wave systems as illustrated Fig. 1.

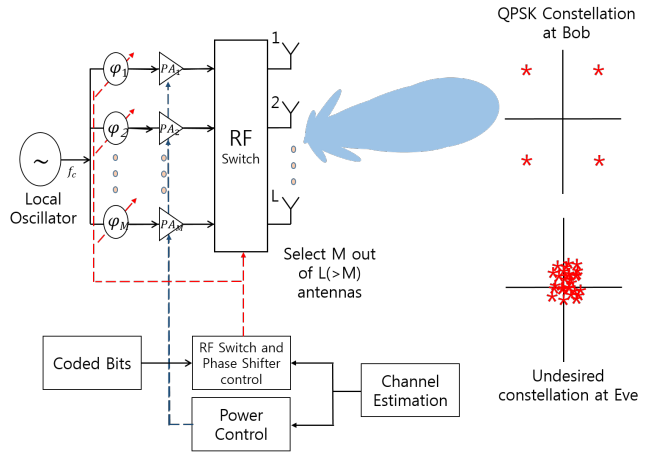

Fig. 1. ASM transmitter for a microwave system

The beamforming vector included the power control parameters for ASM is given by

$$\mathbf{w}(k) = \mathbf{b}(k) \odot \sqrt{\mathbf{p}(k)} \odot \mathbf{h}^*, \tag{2}$$

where $\mathbf{b}(k)$ is an $L \times 1$ random selection vector with $b_i(k) = \{0, 1\}$ and $\sum_{i=1}^{L} b_i(k) = M$. Here, $\mathbf{p}(k)$ is the power control vector which determines the power allocation for transmit antennas and k stands for the time index. Note that in ASM $\mathbf{b}(k)$ is random at each time k. Then, the transmit vector is expressed as

$$\mathbf{x}(k) = \mathbf{w}(k) e^{j\psi(k)}, \tag{3}$$

where $\psi(k)$ denotes the phase offset that depends on confidential data (we assume phase shift keying for signals). Then, the received signal at Bob becomes

$$\begin{aligned} y(k) &= \mathbf{h}^{\mathrm{T}} \mathbf{x}(k) + n(k) \\ &= \mathbf{h}^{\mathrm{T}} \mathbf{w}(k) e^{j\psi(k)} + n(k), \end{aligned} \tag{4}$$

where $n(k) \sim \mathcal{CN}(0, \sigma^2)$ is the background noise at Bob. Furthermore, the received signal at Eve is given by

$$\begin{aligned} z(k) &= \mathbf{g}^{\mathrm{T}} \mathbf{x}(k) + e(k) \\ &= \mathbf{g}^{\mathrm{T}} \mathbf{w}(k) e^{j\psi(k)} + e(k), \end{aligned} \tag{5}$$

where $e(k) \sim \mathcal{CN}(0, \sigma^2)$ is the background noise at Eve.

In ASM, due to random antenna selection, i.e., $\mathbf{b}(k)$, the received signal at Eve looks random. On the other hand, at Bob, due to beamforming based on the CSI at Bob, i.e., $\mathbf{h}^{\mathrm{T}}$, the received signal at Bob is coherently combined and it has much less influence of $\mathbf{b}(k)$.

III. Outage Probabilities of ASM

In this section, we derive the SNRs at Bob and Eve. Since the SNRs are random variables due to random antenna selection in ASM, we consider the outage probabilities for reliability and security.

A. SNRs

In this paper, the power allocation is to maximize Bob's SNR but to keep Eve's SNR low. The SNRs at Bob and Eve, denoted by γ_B and γ_E, respectively, are given by

$$\gamma_B = \frac{|\sum_{l=i_1}^{i_M} h_l w_l|^2}{\sigma^2} \tag{6}$$

and

$$\gamma_E = \frac{|\sum_{l=i_1}^{i_M} g_l w_l|^2}{\sigma^2}, \tag{7}$$

where h_{i_j} and w_{i_j} denote channel and beamforming coefficients for the j-th selected antenna, respectively. Note that the index of the j-th selected antenna is denoted by i_j. For convenience, let $S = \{i_1, ..., i_M\}$. To maximize Bob's SNR, we need to consider the following maximization:

$$\max_{\{w_l\}} \frac{|\sum_{l \in S} h_l w_l|^2}{\sigma^2}. \tag{8}$$

By using Cauchy-Schwarz inequality, the SNR is bounded as follows:

$$\gamma_B \leq \frac{\sum_{l \in S} |h_l|^2 P_T}{\sigma^2}, \tag{9}$$

where $P_T = \sum_l |w_l|^2$ is the total transmit power. When $w_l = \sqrt{\beta} h_l^*$ and $\beta = \frac{P_T}{\sum_l |h_l|^2}$, we can maximize the SNR in (9).

Note that since Alice does not know the channel to Eve, it is not possible for Alice to decide the beamforming coefficients to minimize γ_E. Therefore, we only consider the maximization of γ_B as in (9) for randomly chosen antennas.

B. Outage Probability Analysis

In this subsection, the performance for the beamforming which maximizes Bob's SNR is analyzed in terms of the outage probability. It is noteworthy that the maximum SNR at Bob in (10) is a random variable that depends on the selection of M active antennas, or $\mathbf{b}(k)$, although the total transmit power P_T is fixed.

The outage probability can be used to determine the total transmit power under certain security constraints. The outage event can be differently defined at Bob and Eve. However, for convenience, we use the same SNR threshold to define the outage event at both Bob and Eve. The outage probability at Bob can be given by

$$\begin{aligned} \Phi_B(P_T, \bar{\gamma}) &= \Pr\left(\gamma_B < \bar{\gamma}\right) \\ &= \Pr\left(\sum_{l \in S} |h_l|^2 < \frac{\sigma^2 \bar{\gamma}}{P_T}\right), \end{aligned} \tag{10}$$

where $\bar{\gamma}$ is the threshold SNR. Since $\sum_{l \in S} |h_l|^2$ is a chi-square random variable with $2M$ degrees of freedom, we can show that

$$\begin{aligned} \Phi_B(P_T, \bar{\gamma}) &= F\left(\frac{2\sigma^2 \bar{\gamma}}{P_T}, 2M\right) = R\left(M, \frac{\sigma^2 \bar{\gamma}}{P_T}\right) \\ &= \left(\frac{\sigma^2 \bar{\gamma}}{P_T}\right)^M e^{-\frac{\sigma^2 \bar{\gamma}}{P_T}} \sum_{u=0}^{\infty} \frac{\left(\frac{\sigma^2 \bar{\gamma}}{P_T}\right)^u}{\Gamma(M+u+1)}, \end{aligned} \tag{11}$$

where $F(x, a)$ and $R(a, x)$ are a cumulative distribution function of chi-square distribution and a regularized gamma function, respectively. Here, $\Gamma(x)$ is a gamma function.

With the same threshold SNR, $\bar{\gamma}$, the outage probability at Eve is given by

$$\Phi_E(P_T, \bar{\gamma}) = \mathbb{E}\left[\Pr\left(|\sum_{l \in S} g_l w_l|^2 < \sigma^2 \bar{\gamma} \;\middle|\; \mathbf{w}(\mathbf{h})\right)\right]. \tag{12}$$

Since w_l is independent of g_l and $\sum_l |w_l|^2 = P_T$, we have $\sum_l g_l w_l \sim \mathcal{CN}(0, P_T)$ for given $\{w_l\}$. As a result, it can be shown that

$$\Phi_E(P_T, \bar{\gamma}) = \Pr\left(|\tilde{g}|^2 < \sigma^2 \bar{\gamma}\right), \tag{13}$$

where $\tilde{g} = \sum_l g_l w_l \sim \mathcal{CN}(0, P_T)$. Then, Eve's outage probability is a cumulative distribution function of chi-square distribution with 2 degrees of freedom. From this, we can show that

$$\begin{aligned} \Phi_E(P_T, \bar{\gamma}) &= F\left(\frac{2\sigma^2 \bar{\gamma}}{P_T}, 2\right) \\ &= 1 - e^{-\frac{\sigma^2 \bar{\gamma}}{P_T}}. \end{aligned} \tag{14}$$

We can find that Eve's outage probability is determined by only the total transmit power. The number of selected antennas is not a factor which influences the outage probability at Eve.

IV. Proposed Antenna Selection For Power Efficient Beamforming

In this section, we consider a different antenna selection scheme for ASM to improve the performance by exploiting the difference of the channel gains in micro-wave channels.

In micro-wave channels, since the channel coefficients are random, there are some channel coefficients that have small gains. By excluding the corresponding antennas in ASM, we can improve the performance. In particular, the outage probability at Bob can be improved by removing those antennas in ASM. Suppose that the antennas corresponding to the channel power gain less than $\tau (> 0)$ are removed in ASM. The resulting ASM scheme is referred to as ASM with partial selection in this paper. Throughout the paper, we assume that τ is not too large so that the number of the antennas whose channel power gains are greater than τ is sufficiently large. Let

$$\mathscr{L}_\tau = \{l \mid |h_l|^2 \geq \tau, l = 1, ..., L\}. \tag{15}$$

The average number of the antenna elements in $\mathscr{L}_\tau$ is given by

$$\begin{aligned} \mathbb{E}[|\mathscr{L}_\tau|] &= \mathbb{E}\left[\sum_{l=1}^{L} 1(|h_l|^2 \geq \tau)\right] \\ &= L \Pr(|h_l|^2 \geq \tau) \\ &= L(1 - e^{-\tau}). \end{aligned} \tag{16}$$

The random set for ASM from $\mathscr{L}_\tau$ is now denoted by S_τ. Note that if $\tau = 0$, $S_\tau = S$. Then, the outage probability at Bob is given by

$$\begin{aligned} \tilde{\Phi}_B(P_T, \bar{\gamma}_B, \tau) &= \Pr\left(|\sum_{l \in S_\tau} h_l w_l|^2 < \sigma^2 \bar{\gamma}\right) \\ &= \Pr\left(\sum_{l \in S_\tau} |h_l|^2 < \frac{\sigma^2 \bar{\gamma}}{P_T}\right). \end{aligned} \tag{17}$$

This outage probability is also a cumulative distribution function of chi-square distribution with $2M$ degrees of freedom. In particular, after some manipulations, we can show that

$$\tilde{\Phi}_B(P_T, \bar{\gamma}, \tau) = F\left(\frac{2\sigma^2 \bar{\gamma}}{P_T} - 2M\tau, 2M\right). \tag{18}$$

To find the proper total transmit power, we have to obtain a required total transmit power by using a closed-form expression for the outage probability. For convenience, we denote

a pair of the outage probabilities by $(\tilde{\Phi}_B, \Phi_E) = (\epsilon, 1-\delta)$ for a fixed τ. Here, ϵ and δ are assumed to be sufficiently small. Since it is desirable to keep the outage probability at Eve sufficiently high, δ has to be small. On the other hand, Bob should not have a high outage probability for reliable transmissions, which requires a small ϵ. At Eve, the required total transmit power for a given outage probability becomes

$$P_E(\delta, \bar{\gamma}) = \frac{\sigma^2 \bar{\gamma}}{\ln\left(\frac{1}{\delta}\right)}. \tag{19}$$

Unlike Eve's case, since it is not easy to decide a closed-form expression for the required total transmit power with a fixed outage probability ϵ, we need to rely on a numerical search with a good initial value. For good initial values, we can use the inequalities for the regularized gamma function in [13] as follows:

$$(1-e^{-s_a x})^a < \frac{\gamma(a,x)}{\Gamma(a)} < (1-e^{-r_a x})^a, \tag{20}$$

where $r_a = 1$, $s_a = [\Gamma(1+a)]^{-1/a}$ for $a > 1$. Then, the initial values are given by

$$\begin{aligned} x_i(\epsilon, \bar{\gamma}) &= \frac{\sigma^2 \bar{\gamma}}{\sqrt[M]{\Gamma(1+M)} \ln \frac{1}{(1-\sqrt[M]{\epsilon})} + M\tau} \\ x_u(\epsilon, \bar{\gamma}) &= \frac{\sigma^2 \bar{\gamma}}{\ln \frac{1}{(1-\sqrt[M]{\epsilon})} + M\tau}, \end{aligned} \tag{21}$$

where $x_i(\epsilon, \bar{\gamma}) < \tilde{P}_B(\epsilon, \bar{\gamma}) < x_u(\epsilon, \bar{\gamma})$. We can approximate the required total transmit power $(\tilde{P}_B(\epsilon, \bar{\gamma}))$ by using the bisection method with the initial values. Then, we can find a feasible point ϵ° satisfying $\tilde{P}_B(\epsilon, \bar{\gamma}) = P_E(\delta, \bar{\gamma})$ with $\epsilon = \delta = \epsilon^\circ$.

Note that as shown in (17), $P_E(\delta, \bar{\gamma})$ is an increasing function of δ. On the other hand, $\tilde{P}_B(\epsilon, \bar{\gamma})$ is a decreasing function of ϵ. Thus, there exists $\epsilon^\circ = \epsilon = \delta$ with $\tilde{P}_B(\epsilon, \bar{\gamma}) = P_E(\delta, \bar{\gamma})$. Furthermore, since $\tilde{P}_B(\epsilon, \bar{\gamma})$ decreases with τ, we can expect that ϵ° can decrease with τ as $P_E(\delta, \bar{\gamma})$ is independent of τ. In other words, we can have a better security (a smaller δ) and reliability (a smaller ϵ) by increasing τ in the proposed scheme.

V. Simulation Results

In this section, we present simulation results with quadrature phase shift keying (QPSK) modulation for signaling with $\psi(k)$. We assume that the noise variance is normalized as $\sigma^2 = 1$.

Fig. 2 shows the outage probability for different values of total transmit power when $L = 100, M = 3, \bar{\gamma} = 10$ dB, and $\tau = 0.15$. As the total transmit power increases, Bob and Eve have better performances in terms of outage probability, i.e., the outage probabilities decrease with P_T. However, we can see that the outage probability at Eve is much higher than that at Bob. In addition, using ASM with partial selection, the outage probability at Bob can be further reduced.

Fig. 3 shows the outage probability for different values of M when $L = 100, P_T = 10$ dB, $\bar{\gamma} = 10$ dB, and $\tau = 0.15$. As the number of active antennas increases, only Bob has better performance. Regardless of the number of active antennas, Eve's outage probability remains unchanged. Thus, it would be desirable to have a large M. However, if M is too large, the randomness of ASM decreases, which may not be desirable as Eve can use it for better eavesdropping by analyzing ASM patterns.

Fig. 4 shows the total transmit power that is required to satisfy given ϵ and δ for Bob and Eve, respectively, when $L = 100, M = 10, \bar{\gamma} = 10$ dB, and $\tau = 0.35$. As mentioned earlier, there exists $\epsilon^\circ = \epsilon = \delta$ for a certain total transmit power. We can see that the performance can be improved as the value of ϵ° is lower in ASM with partial selection than that in conventional ASM.

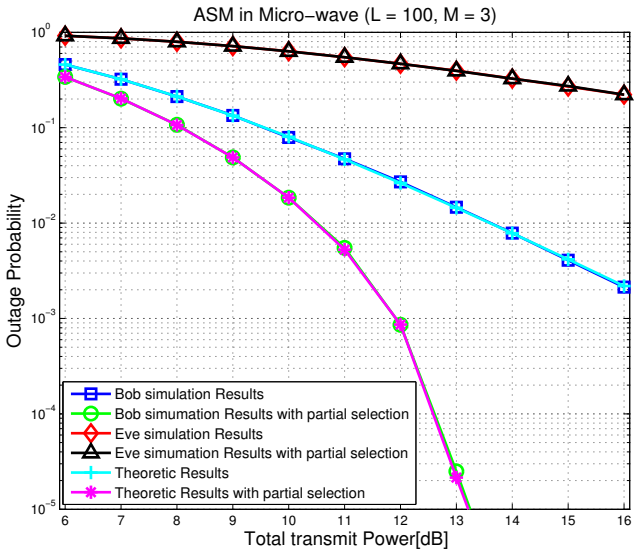

Fig. 2. Total transmit power versus outage probability

VI. Conclusion

In this paper, we studied beamforming for ASM in micro-wave systems. Due to different channel gains under rich scattering environments in micro-wave systems, for ASM, we considered effective power allocation with beamforming. To improve the performance of ASM, we proposed partial selection in random antenna selection by removing some antennas corresponding to weak channel gains. We derived the outage probabilities at Bob and Eve to see the performance. It was shown that Bob can have a sufficiently low outage probability, while Eve suffers from a high outage probability by ASM. It was also observed that a lower outage probability at Bob has been obtained by ASM with partial selection.

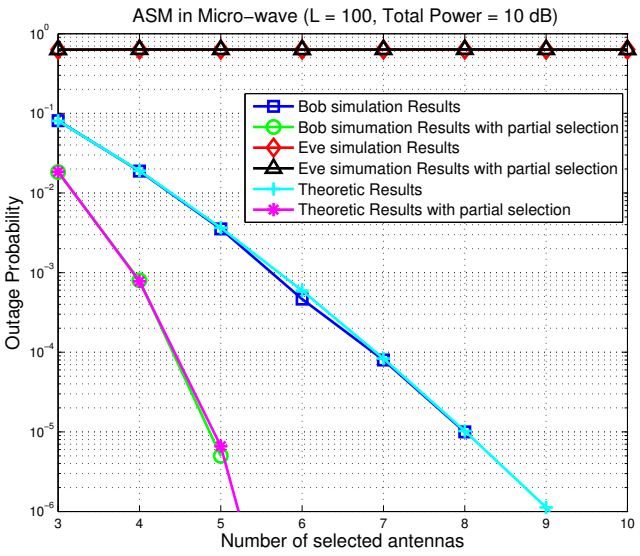

Fig. 3. Number of selected antennas versus outage probability

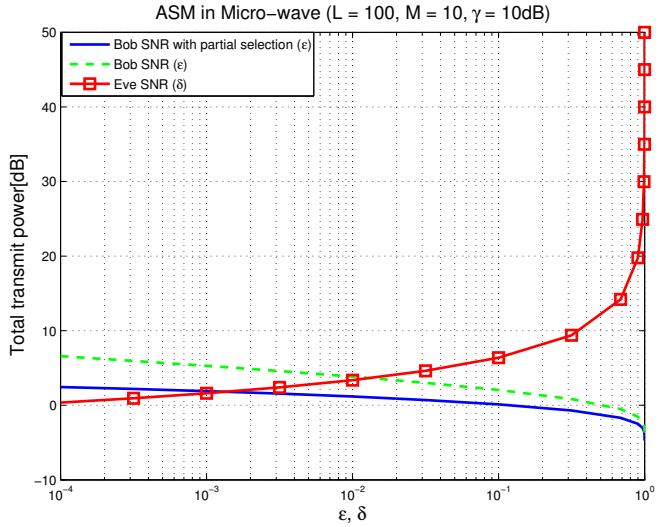

Fig. 4. Target outage probability versus required SNR

ACKNOWLEDGMENT

This work was supported by Agency for Defense Development (the title of the project is PHY/MAC-NETWORK Technologies Against Jamming Attack and Eavesdropping).

REFERENCES

[1] Y. Liang, H. V. Poor, *et al.*, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[3] C. E. Shannon, "Communication theory of secrecy systems*," *Bell system Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 8, pp. 4961–4972, 2011.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180–2189, 2008.

[6] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *Antennas and Propagation, IEEE Transactions on*, vol. 57, no. 9, pp. 2633–2640, 2009.

[7] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *Antennas and Propagation, IEEE Transactions on*, vol. 58, no. 5, pp. 1545–1550, 2010.

[8] T. Hong, M.-Z. Song, and Y. Liu, "RF directional modulation technique using a switched antenna array for physical layer secure communication applications," *Progress In Electromagnetics Research*, vol. 116, pp. 363–379, 2011.

[9] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 4, pp. 619–625, 2013.

[10] J. Choi, J. Ha, and H. Jeon, "Physical layer security for wireless sensor networks," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*, pp. 1–6, IEEE, 2013.

[11] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *Communications, IEEE Transactions on*, vol. 61, no. 8, pp. 3231–3245, 2013.

[12] C. Rusu, N. Gonzalez-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*, pp. 2914–2918, IEEE, 2015.

[13] H. Alzer, "On some inequalities for the incomplete gamma function," *Mathematics of Computation of the American Mathematical Society*, vol. 66, no. 218, pp. 771–778, 1997.