The Guidebook of the PLS toolbox for CCPS

Ozan Alp Topal, Mehmet Özgün Demir, Zekai Liang, Ali Emre Pusane, Guido Dartmann,
Gerd Ascheid, and Güneş Karabulut Kurt

March 2020

1 Introduction

In this guidebook, we present the details of the theoretical aspects of the proposed CCPS framework, with the title: “A Physical Layer Security Framework for Cognitive Cyber Physical Systems”. The simulation environment are also given with a comparison of simulation and test results. With this toolbox, the readers can update the utility weights, which are provided in the Table 4, to find the best PLS policy for other application scenarios.

In this guidebook, we firstly explain the simulation system model with possible attack scenarios. After that the available physical layer security (PLS) policies are given. The performance metric is also presented in details in Section 4. The simulation results are shown with test results after calculating the utility values in Section 5.

2 Simulation Model

Our simulation setup mainly consists of four nodes: the transmitter (Alice), the receiver (Bob), the eavesdropper (Eve), and the jammer, as described in Figure 1. Considering the cognitive cyber physical systems (CCPS) framework, Alice and Bob correspond to the control center and the sensor nodes, respectively.

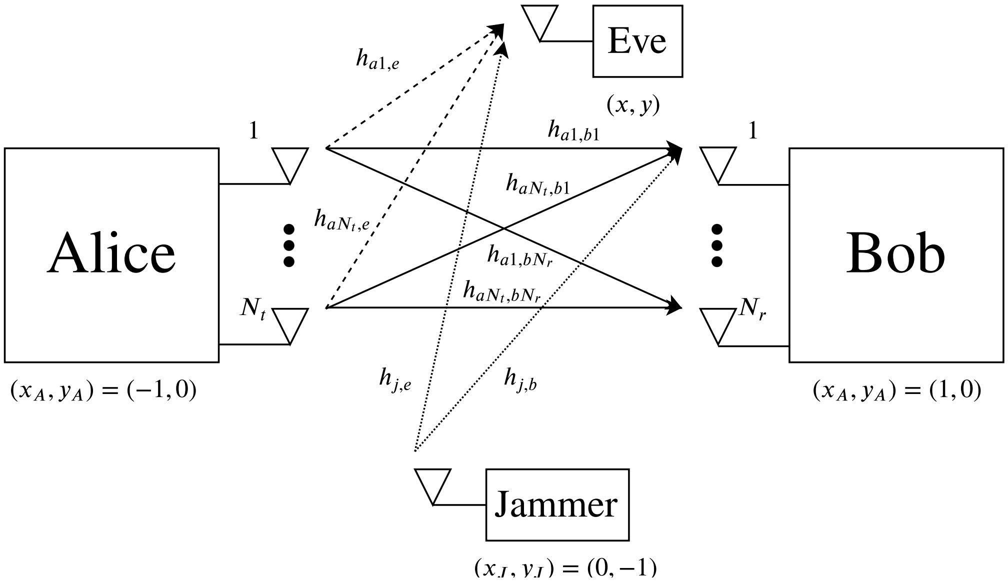


Figure 1: The considered system model for the simulations.

2.1 Attacker Model

By including a jammer to the simulation model, we consider the co-existence of two different attacks. We also analyze different jamming power and eavesdropper position scenarios, as given in Table 1.

Table 1: Considered jamming power levels and expected location values for the eavesdropper.

Jamming Power (dB)		Expected Eavesdropper Position	
P_{J1}	none	p_{E1}	$x_E = -1, y_E = 0$
P_{J2}	0	p_{E2}	$x_E = 0, y_E = 0$
P_{J3}	5	p_{E3}	$x_E = 1, y_E = 0$
P_{J4}	10		

Note that, while Alice, Bob, and the jammer are assumed to be positioned, as shown in the Figure, we model the position of the eavesdropper as a 2D Gaussian random variable as detailed in Section 4. Uncorrelated Rayleigh channel fading is assumed between each transmitter-receiver antenna pairs. The path loss exponent is assumed as $PL = 2$. The environment or surface S is defined in Cartesian coordinates (x, y), where $-2m < x < 2m$ and $-2m < y < 2m$. The message transmission power of Alice (denoted as P_m in Section 3) is assumed to be fixed at 5dB.

3 PLS policies

We consider four different PLS policies: subcarrier based artificial noise (SC-AN), full-duplex artificial interference (FD-AI), beamforming, and artificial noise with beamforming (B-AN). Note that enlisted security policies have different requirements; therefore, some security policies may not be practiced to limited resources. The security policies are modeled with the parameters given in Table 2.

While the last two policies exploit multiple antenna characteristics, the first policy utilizes the pilot subcarriers at orthogonal frequency division multiplexing (OFDM), and the second policy uses full-duplex transmission. We will initially present a detailed system model and later explain the signal-to-noise ratio (SNR) expressions for the enlisted policies. Then, we will provide a comparison of the enlisted PLS policies.

Table 2: Simulation parameters for each PLS policy.

Policy	$N_t \times N_r$	Artificial noise power in dB(P_w)
Subcarrier based AN	1×1	0,5,10
Full-duplex based AI	1×2	0,5,10
Beamforming	2×1	none
Beamforming with AN	2×2	0,5,10

1) Subcarrier Based Artificial Noise: As mainly described in [1], subcarrier based artificial noise is utilized with single-input-single-output (SISO) OFDM system. In this case, $N_t = 1$ and $N_r = 1$ considering the Figure 1. At Alice, the discrete time baseband representation of the transmitted signal can be given by

$$x(n) = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} X(k) e^{j2\pi kn/K}, \tag{1}$$

where K is the number of subcarriers. The transmitted message symbols are constructed as

$$X(k) = \begin{cases} X_{m,p}(q) \ , \ k = ql \\ X_w(q) \ , \ k = ql + 1 \\ X_m(k) + X_w(q) \ , \ ql + 1 < k < (q+1)l \end{cases}, \tag{2}$$

for $q = 0, 1, \cdots, Q$ and $Ql = K - 2$. $X_m(k)$ denotes the transmitted message for an OFDM symbol, and $X_w(k)$ denotes the transmitted artificial noise term for an OFDM symbol. Note that, we use same $X_w(q)$ protecting $l - 1$ number of data symbols and than update the noise term. Besides Alice, we also assume the existence of a jammer node in the environment. The jamming signal can be given by $x_j(n) \sim \mathcal{CN}(0, P_j)$, where $\mathcal{CN}(\mu, \sigma^2)$ denotes circularly symmetric complex normal distribution with mean μ and variance σ^2. Considering uncorrelated Rayleigh flat fading channel, the received signal at Bob becomes

$$y_b(n) = x(n) * h_{ab}(n) + x_j(n) * h_{jb}(n) + z(n), \tag{3}$$

where $h_{ab}(n) = h_{ab}\delta(n)$, and $h_{ab} \sim \mathcal{CN}(0, \frac{1}{d_{ab}^{PL}})$. $\delta(n)$ denotes the unit impulse function, PL denotes the path loss exponent, and $z(n)$ denotes the additive white Gaussian noise (AWGN) component with $z(n) \sim \mathcal{CN}(0, N_0)$. After the DFT operation at Bob, the received signal becomes

$$Y_b(k) = h_{ab}X_m(k) + h_{ab}X_w(k) + h_{jb}X_j(k) + Z(k), \tag{4}$$

where $h_{jb} \sim \mathcal{CN}(0, \frac{1}{d_{jb}^{PL}})$. In order to cancel the artificial noise term at Bob, let us define the artifical noise term for $k = 1, l + 1, \ldots, Ql + 1$ as

$$Y_{w,p}(k) = h_{ab}X_w(k) + h_{jb}X_j(k) + Z(k). \tag{5}$$

If we subtract this term by the rest of the subcarriers at received signal, we can find the received message signal part as

$$Y_m(k) = h_{ab}X_m(k) + h_{jb}X_j(k) - h_{jb}X_j(q) + Z(k) - Z(q). \tag{6}$$

Than, the SINR at Bob for subcarrier based artificial noise (SC-AN) policy becomes

$$SINR_b^{scAN} = \frac{|h_{ab}|^2 P_m}{2|h_{jb}|^2 P_j + 2N_0}, \tag{7}$$

where P_m symbolizes the power of the message signal. Due to the artificial noise cancellation operation, the effect of jamming and noise terms become more distorting.

The received signal at Eve similarly becomes

$$y_e(n) = x(n) * h_{ae}(n) + x_j(n) * h_{je}(n) + z(n), \tag{8}$$

where $h_{ae}(n) = h_{ae}\delta(n)$, and $h_{ae} \sim \mathcal{CN}(0, \frac{1}{d_{ae}^{PL}})$. Similarly, $h_{je}(n) = h_{je}\delta(n)$, and $h_{je} \sim \mathcal{CN}(0, \frac{1}{d_{je}^{PL}})$. After DFT operation, the received signal at Eve becomes,

$$Y_e(k) = h_{ae}X_m(k) + h_{ae}X_w(k) + h_{je}X_j(k) + Z(k). \tag{9}$$

The SINR at Eve for subcarrier based artificial noise (sc-AN) policy becomes

$$SINR_e^{scAN} = \frac{|h_{ae}|^2 P_m}{|h_{ae}|^2 P_w + |h_{je}|^2 P_j + N_0}. \tag{10}$$

2) Full-Duplex Based Artificial Interference: Another popular policy among PLS is full-duplex deployment as shown in [1] and [2]. In our simulations, we consider that Bob utilizes full duplex transmission;therefore, $N_t = 1$, $N_r = 2$ in Figure 1. Than, under uncorralated Rayleigh fading channel assumption, the baseband discrete-time representation of the received signal at Bob can be described by

$$y_b(n) = h_{ab}x_a(n) + h_{bb}w_b(n) + h_{jb}x_j(n) + z(n), \tag{11}$$

where $x_a(n)$ is the message signal transmitted by Alice, $w_b(n) \sim \mathcal{CN}(0, P_w)$ is the artificial interference generated by Bob and $z(n) \sim \mathcal{CN}(0, N_0/2)$ is the AWGN at Bob. $h_{bb} \sim \mathcal{CN}(0, 1)$ is assumed to be perfectly known by Bob. Since Bob knows $w_b(n)$ and h_{bb}, we assume perfect self-interference-cancellation (SIC) at Bob. Than the received signal becomes

$$r_b(n) = h_{ab}x_a(n) + h_{jb}x_j(n) + z(n). \tag{12}$$

Than, the SINR at Bob is described by

$$SINR_b^{ai} = \frac{|h_{ab}|^2 P_m}{|h_{jb}|^2 P_j + N_0}. \tag{13}$$

The received signal at Eve is described by

$$y_e(n) = h_{ae}x_a(n) + h_{be}w_b(n) + h_{je}x_j(n) + z(n), \tag{14}$$

where $h_{be} \sim \mathcal{CN}(0, \frac{1}{d_{be}^{PL}})$. Since the eavesdropper cannot apply SIC, the SINR expression at Eve becomes

$$SINR_e^{ai} = \frac{|h_{ae}|^2 P_m}{|h_{be}|^2 P_w + |h_{je}|^2 P_j + N_0}. \tag{15}$$

As it can be seen from SINR expressions, this policy provides better security at locations close to Bob.

3) Beamforming: Exploiting the channel randomness and diversity obtained from the multiple antennas, beamforming is exhaustively applied in PLS works as detailed in [3]. In our simulation model, we consider $N_t = 2$ and $N_r = 1$. The received signal at Bob is given by

$$y_b(n) = \mathbf{h_{ab}}^T \Theta x_a(n) + h_{jb}x_j(n) + z(n), \tag{16}$$

where $\mathbf{h_{ab}} = [h_{ab}(1), h_{ab}(2)]^T$ denotes the uncorrolated Rayleigh channel coefficients from the transmitting antennas and $\Theta = [\theta_1, \theta_2]^T$ denotes the beamforming vector. Assuming the channel fading coefficients are perfectly known at Alice, we select the beamforming coefficient vector as

$$\Theta = \frac{\mathbf{h_{ab}}^\dagger}{||\mathbf{h_{ab}}||},$$

where $(\cdot)^\dagger$ denotes the complex conjugate transpose (Hermitian) operation [3]. The SINR value at Bob of the resulting signal becomes

$$SINR_b^b = \frac{||\mathbf{h_{ab}}||^2 P_m}{|h_{jb}|^2 P_j + N_0}. \tag{17}$$

The received signal at Eve can be given by

$$y_e(n) = \mathbf{h_{ae}}^T \Theta x_a(n) + h_{je}x_j(n) + z(n). \tag{18}$$

The SINR expression at Eve is described by

$$SINR_e^b = \frac{||\mathbf{h_{ab}}^\dagger \mathbf{h_{ae}}|| P_m}{|h_{je}|^2 P_j + N_0} \tag{19}$$

Note that, by selecting a beamforming vector in line with the channel coefficients between Alice and Bob, we deteriorate the performance of the received signal at all points except Bob's.

4) Beamforming with Artificial Noise: Artificial noise is the most common PLS metric and generally is utilized with beamforming since the transmitter node is already assumed to be equipped with multiple antennas [4], [5]. The received signal at Bob is described by

$$y_b(n) = \mathbf{h_{ab}}^T \Theta x_a(n) + \mathbf{h_{ab}}^T \Gamma x_w(n) + h_{jb}x_j(n) + z(n), \tag{20}$$

where $\Gamma \in \mathcal{N}(\mathbf{h_{ab}}^T)$ and $x_w(n) \sim \mathcal{CN}(0, P_w/2)$. $\mathcal{N}(\mathbf{c})$ denotes an orthonormal vector to the vector $\mathbf{c}$. Therefore, $\mathbf{h_{ab}}^T\Gamma = 0$ and the received signal can be simplified to

$$y_b(n) = \mathbf{h_{ab}}^T\Theta x_a(n) + h_{jb}x_j(n) + z(n). \tag{21}$$

The SINR expression at Bob becomes

$$SINR_b^{b,an} = \frac{||\mathbf{h_{ab}}||^2 P_m}{|h_{jb}|^2 P_j + N_0}. \tag{22}$$

The received signal at Eve can be described by

$$y_e(n) = \mathbf{h_{ae}}^T\Theta x_a(n) + \mathbf{h_{ae}}^T\Gamma x_w(n) + h_{je}x_j(n) + z(n). \tag{23}$$

The SINR expression at Eve becomes

$$SINR_e^{b,an} = \frac{||\mathbf{h_{ab}}^\dagger\mathbf{h_{ae}}||P_m}{\mathbf{h_{ae}}\Gamma\Gamma^\dagger\mathbf{h_{ae}}^\dagger P_w + |h_{je}|^2 P_j + N_0}. \tag{24}$$

We obtain ergodic secrecy capacity and ergodic secrecy pressure expressions in line with the given SINR expressions for each PLS policy. Figure 2 provides a rough comparison of the security performance of different PLS policies. An overall comparison of the advantages and disadvantages of the provided policies can be summarized as in Table 3.

Table 3: A comparison of the considered PLS policies.

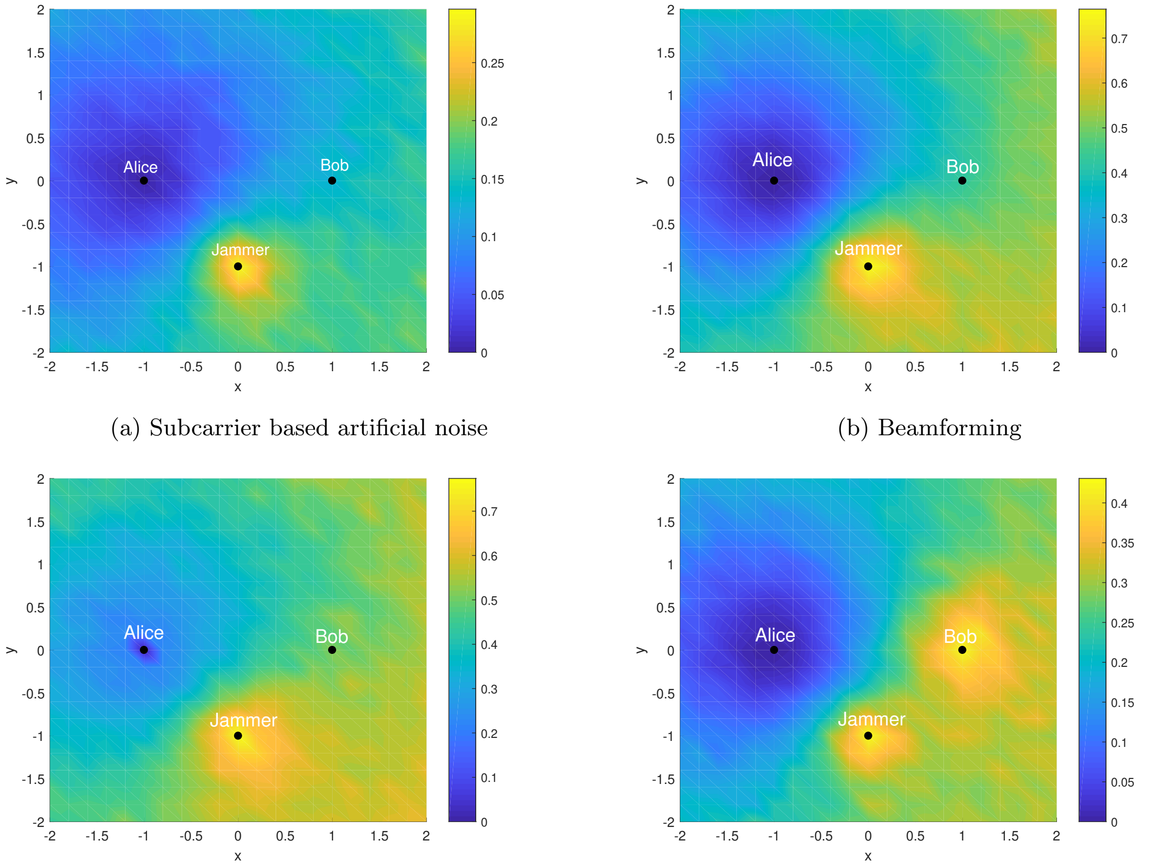
		SC-AN	AI	Beamforming	AN
Requirements	CSI at Alice	x	x	✓	✓
	Multiple antenna at Alice	x	x	✓	✓
	Multiple antenna at Bob	x	✓	x	x
	Artificial noise	✓	✓	x	✓
Performance	Security	Low	Modarate	High	High
	QoS	Moderate	Moderate	High	High
	Cost	Low	Moderate	High	High

Since several 5G deployments would require different solutions, a single security policy cannot establish the best performance for each deployment. Therefore, we first provide utility as a metric to compare different PLS solutions, while the users are allowed to change the importance level of various performance metrics. Note that, more complex or hybrid policies may also be included in the framework in line with the capabilities of the CCPS network. For the sake of simplicity and clarity, we have limited the security policies with the most comparable and popular four policies.

4 Security Metric

As a first step, ergodic secrecy capacity of each point (x, y) of the surface S is obtained. This step provides us a secrecy map of the surface S for the corresponding security policy. After that, expectation operation is applied over the surface S. The location of the eavesdropper is assumed to be a 2D Gaussian random variable since the surface might contain different physical measures in different areas. For example, considering a factory environment, the mean of the Gaussian distribution may be assumed as the blind spot of the security cameras. As depicted in Fig. 2, Alice, Bob, and a jammer are located at (x_A, y_A), (x_B, y_B), (x_J, y_J), respectively, on the surface S, where the distance from the i^{th} node to the j^{th} is denoted by $d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)}$ for $i, j \in \{A, B, J\}$. The position of eavesdropper is unknown; therefore, it will be denoted by (x, y). The secrecy capacity can be represented by

$$C_{sec}(x, y) = \max\{0, (C_B - C_E(x, y))\}, \tag{25}$$



(a) Subcarrier based artificial noise

(b) Beamforming

(c) Beamforming with artificial noise

(d) Full duplex based artificial interference at Bob

Figure 2: Secrecy maps of the corresponding PLS policies. Secrecy capacity values considering each eavesdropper position are indicated by corresponding colors given in the legends. During simulations, the signal power at Alice is assumed 5dB. The signal power of jammer is assumed 5dB. Positions of Alice, Bob, and jammer are fixed to $(x_A = -1, y_A = 0)$, $(x_B = 1, y_B = 0)$ and $(x_J = 0, y_J = -1)$, respectively.

where C_B and $C_E(x, y)$ are respectively the channel capacities between Alice and Bob, and between Alice and Eve. The capacity of Bob's channel can be given as

$$C_B = \frac{1}{2} \log\left(1 + \mathrm{SINR}_B\right), \tag{26}$$

and the Eve's channel capacity is

$$C_E(x, y) = \frac{1}{2} \log\left(1 + \mathrm{SINR}_E(x, y)\right), \tag{27}$$

where SINR_j denotes signal-to-interference-noise-ratio (SINR) at j^{th} node. Note that, the capacity of a generic (x, y) point is given since the location of the eavesdropper is unknown. Since the secrecy capacity depends on the mutually independent, i.i.d. channel fading coefficients $h_{ae}, h_{be}, h_{je}, h_{ab}, h_{jb}$, the ergodic secrecy capacity can be given as

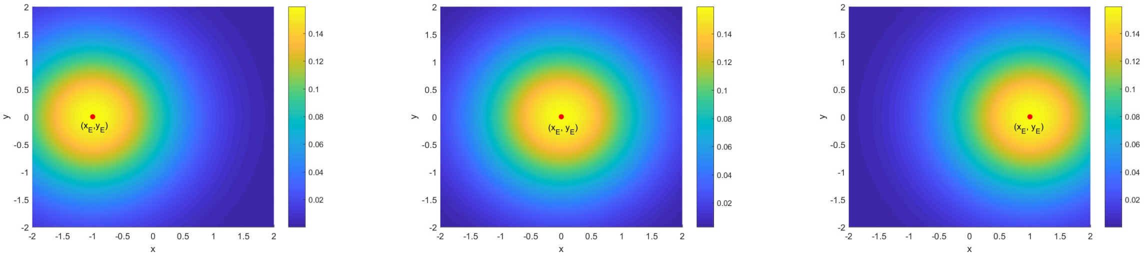
$$\tilde{C}_{sec}(x, y) = \mathbb{E}_{|h_{ae}|^2, |h_{be}|^2, |h_{je}|^2, |h_{ab}|^2, |h_{jb}|^2}\left[C_{sec}(x, y)\right], \tag{28}$$

where $\mathbb{E}\{.\}$ denotes the expectation operator. Note that, ergodic secrecy capacity is also defined for a generic (x, y) point. Calculating ergodic secrecy capacity for each point on the surface S would result in calculating the secrecy map of the surface, as illustrated in Fig. 2. In this figure, we provide secrecy maps for our chosen security policies. Each policy provides a different level of security at different points on the surface. For example, as depicted in Fig. 2d, artificial interference at Bob, provides much higher ergodic secrecy capacity near Bob in comparison with other policies, because the noise signal is transmitted from Bob. Therefore, the knowledge on the position of the eavesdropper is important to decide the best performing security policy.

As indicated in Section V of [6], even though, we cannot estimate the exact position of the eavesdropper, we may define a suspicious region which is highly likely to eavesdrop. For example, in a factory environment, some areas might be more accessible to guests and hard to detect from security cameras. When we move away from a suspicious area, we can assume that the likelihood of eavesdropping activity also decreases. Considering this perspective, we can weigh the ergodic secrecy capacity for each (x, y) generic point by the probability of eavesdropper's existence at that point. Then, the ergodic secrecy pressure of the surface S can be given by

$$P_{sec} = \int\int_S \gamma(x,y)\tilde{C}_{sec}(x,y)dxdy, \tag{29}$$

where $\gamma(x, y)$ is the probability density function of the presence of Eve at a point (x, y) on the surface. As in Eq. (30) of [6], we consider the case where the probability density function of the eavesdropper's location is Gaussian distributed with $\gamma(x,y) = \frac{1}{\sqrt{2\sigma_e^2}} e^{\frac{-(x-x_E)^2-(y-y_E)^2}{2\sigma_E^2}}$.



(a) $x_E = -1, y_E = 0$

(b) $x_E = 0, y_E = 0$

(c) $x_E = 1, y_E = 0$

Figure 3: The probability distribution functions of the presence of eavesdropper at a point on the surface with corresponding (x_E, y_E) values, where Alice is located at $x_A = -1, y_A = 0$, Bob is located at $x_B = 1, y_A = 0$, and jammer is located at $x_j = 0, y_j = 1$.

In order to compare the performance of PLS policies in different suspicious eavesdropper locations, we consider three different (x_E, y_E) position cases in simulations, as depicted in Fig. 3. Three cases respectively indicate that the region around Alice, Bob, and the midpoint are more prone to eavesdropper attacks than other regions. Therefore, ergodic secrecy capacity values at that points depict the security performance of the system better than other points. Then, the ergodic secrecy pressure provides us an observation of the security level of the surface S.

Note that, ergodic secrecy pressure provides the most realistic security analysis in the PLS literature. When we consider ongoing metric research, a better representation might be available in future practice. Our proposed framework is adaptable in the sense that security, QoS, or cost metrics can easily be updated without changing the structure of the framework.

5 Utility Calculation

In order to deploy to our CCPS framework, we obtain a utility value for each policy before a transmission cycle, and than we select best performing policy. The utility can be given by

$$U^i = w_{sec}\text{Security} + w_{QoS}\text{QoS} + w_{cost}(1 - \text{Cost}), \tag{30}$$

where $i \in \{scAN, fdAI, b, bAN\}$ denotes subcarrier based artificial noise, full-duplex based artificial interference, beamforming, and artificial noise with beamforming, respectively. $w_{sec}, w_{QoS}, w_{cost}$ are the coefficients of the security, quality of service and cost dimensions of the CCPS framework, and $w_{sec} + w_{QoS} + w_{cost} = 1$. Considering different 5G deployment cases, we have assigned four different weightings as in Table 4. The utility weights are equally chosen in Table 4 (a) for C_1 since drone swarms require high QoS, security, and low cost at the same time in military or commercial applications. As the second case, ultra-reliable low latency communication (URLLC) and vehicle-to-everything (V2X) communication systems are chosen. To deploy these applications with very high reliability and very low end-to-end latency, in the orders of 10^{-7} error rate and a few milliseconds, respectively, the highest weight is assigned for QoS dimension sufficient security against eavesdroppers [7]. In the third case, equal security and cost weights are assigned for mMTC and smart grid applications, which may consist of a tremendous amount of nodes with limited energy simultaneously operating with low data rates. As a security threat, node capture, node outage, and false node attacks can be performed in mMTC systems. There are also high risks for privacy in smart grid systems. Finally, security is the most vital dimension regarding our CCPS framework in the case of C_4 due to the inherent security and privacy risks of the medical CCPS applications with sensitive medical data of individuals. Because of the limited batteries of wireless medical applications, they are also vulnerable to DoS attacks [8]. Therefore assigned weight for cost dimension should be sufficiently high in C_4.

Table 4: Assigned security, QoS and cost weights in utility calculation for four different 5G deployment cases.

	Utility Weights			Applications
	w_{sec}	w_{QoS}	w_{cost}	
C_1	0.33	0.33	0.33	Drone swarms
C_2	0.3	0.6	0.1	URLLC, V2X
C_3	0.4	0.2	0.4	mMTC, Smart Grid
C_4	0.3	0.1	0.6	Health networks

In order to pave the way for future beyond 5G applications, readers can assign the utility weights and determine best performing security policy. In the following, we describe the parameters utilized for each dimension and the normalization operation.

Security: Note that, before establishing the CCPS framework, the ergodic secrecy capacity of each point on the chosen environment is separately calculated considering each available security policy. After calculating ergodic secrecy capacity, the ergodic secrecy pressure of the environment is calculated as detailed in 4. As a result of the calculations of secrecy pressure values for each security policy, the security is normalized by

$$\text{Security}_i = \frac{P^i_{sec}}{\max_i(P^i_{sec})}. \tag{31}$$

QoS: The principal metric for QoS is selected as the SINR value at Bob. Note that, delays and jitters are generally part of the QoS; however, for the sake of simplicity, we will only focus on the SINR at Bob as the central QoS indicator. Similar to security calculation, we normalize the QoS metric by

$$\text{QoS}_i = \frac{SINR^i_b}{\max_i(SINR^i_b)}. \tag{32}$$

Cost: The main components of the cost in the simulations are the artificial noise power, the number of transmitter antennas, and the number of receiver antennas. In order to calculate the cost, we initially obtain the weighted average of these components similarly to [9] by

$$\text{Total Cost} = w_{P_w}(\text{Noise Power}) + w_{Tx}(\#\text{Transmitter antenna}) + w_{Rx}(\#\text{Receiver antenna}). \tag{33}$$

For the sake of simplicity, we select $w_{P_w} = w_{Tx} = w_{Rx}$ and $w_{P_w} + w_{TxA} + w_{RxA} = 1$. Following this, we utilize same normalization approach as in security and QoS by

$$\text{Cost} = \frac{\text{Total Cost}^i}{\max_i(\text{Total Cost}^i)}. \tag{34}$$

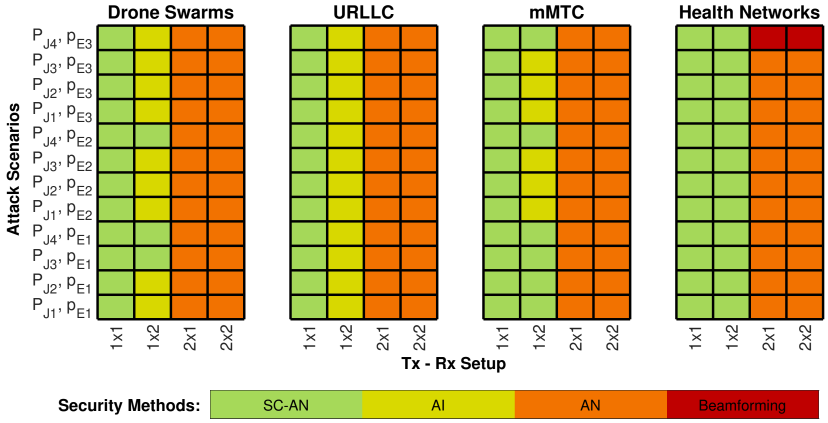


Figure 4: Selected security policies considering different attack and antenna orientation for four different 5G scenarios.

5.1 Simulation and Test Results

After calculating utility values for each policy, the control center selects the best performing policy prior to data transmission and sends the control context to the sensor node. The simulation results under different attack scenarios and 5G deployments are given in Figure 4. Note that the given TX-RX antenna setup indicates the resources. As an example, the SC-AN policy is still applied with a single transmit and receiver antenna, even though both transmitter and receiver have 2 antennas. Results mainly indicate that selected security policy does not affect by changing jamming powers. However, the expected position of the eavesdropper impacts the selected policy. For example, in the 1×2 antenna deployment, AI policy is favorable as the expected location of eavesdropper approaches to Bob, because the disruptive noise is emitted from Bob in AI policy. Another observation is that antenna based approaches (beamforming and AN) provide higher security and QoS levels than other policies. Therefore, for the security and QoS critical applications, their selection becomes favorable.

Besides simulations, we have updated our test results by utilizing the same parameters in the simulations. To measure SINR levels at the receiver and Bob, we use the connection between EVM and SINR expressions. Due to the difficulties in the real-time systems, we do not include jamming attacks as in P_{J1} and assume the expected eavesdropper position as in p_{E2}. Figure 5 provides a comparison of utility values in simulations and tests considering two different PLS policies. As can be seen from the figure, the test results vary from the simulations because of the real-time channel estimation errors. As expressed in the manuscript, estimation errors deteriorate the performance of the PLS policies. Therefore, any optimization attempt in the cognitive CCPS frameworks should consider the estimation errors as highlighted in Section V of the manuscript.

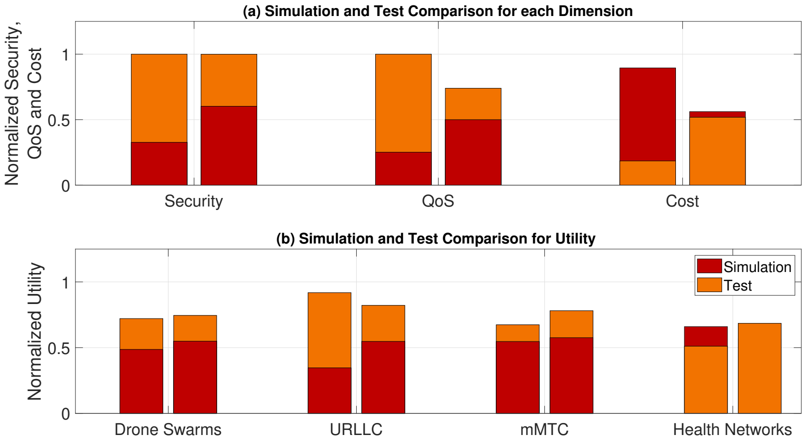


Figure 5: Selected security policies considering different attack and antenna orientation for four different 5G scenarios.

References

[1] S. Gökçeli, O. Cepheli, S. T. Basaran, G. K. Kurt, G. Dartmann, and G. Ascheid, "How effective is the artificial noise? Real-time analysis of a PHY security scenario," in *Proceedings of the GLOBECOM Workshops*, Dec 2017, pp. 1–7.

[2] Ö. Cepheli, S. Tedik, and G. Karabulut Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE Communications Letters*, vol. 18, no. 6, pp. 1075–1078, June 2014.

[3] Z. Sheng, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Beamforming optimization for physical layer security in MISO wireless networks," *IEEE Transactions on Signal Processing*, vol. 66, no. 14, pp. 3710–3723, July 2018.

[4] R. Negi and S. Goel, "Secret communication using artificial noise," in *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.*, vol. 3, Sep. 2005, pp. 1906–1910.

[5] Xiangyun Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *2009 3rd International Conference on Signal Processing and Communication Systems*, Sep. 2009, pp. 1–5.

[6] L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang, "A new metric for measuring the security of an environment: The secrecy pressure," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3416–3430, May 2017.

[7] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 6–11, 2019.

[8] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[9] M. Alia, M. Lacoste, R. He, and F. Eliassen, "Putting together qos and security in autonomic pervasive systems," in *Proceedings of the 6th ACM workshop on QoS and security for wireless and mobile networks*, 2010, pp. 19–28.