Secure Joint Communications and Sensing using Chirp Modulation

Saumya Dwivedi, Marco Zoli, André N. Barreto, Padmanava Sen
Barkhausen Institut, Dresden, Germany
saumya.dwivedi, marco.zoli, andre.nollbarreto, padmanava.sen@barkhauseninstitut.org

Gerhard Fettweis
Technische Universität Dresden
gerhard.fettweis@tu-dresden.de

***Abstract*—Joint sensing and communications is likely to be one of the new features in upcoming 6G systems. With this in mind, we propose a chirp-based waveform that is adequate for both of these purposes. We analyse its performance in two different scenarios, automotive and robotics for industry 4.0, with stochastic radio channel. Moreover, we show how to increase the system security by generating encryption keys from the random common channel using this waveform. To increase the entropy of the key, we develop a wideband approach, based on filterbank filtering.**

I. Introduction

So far radar sensing and communications employ different systems with dedicated spectrum and equipment, although both functionalities rely on the same physical principles of electromagnetic wave propagation. Hence, there is nothing in the way of using the same spectrum and hardware for both purposes, increasing spectrum availability and lowering equipment costs and energy consumption. With this in mind, joint radar and communication (RadCom) systems have been recently proposed [1], [2], and joint sensing and communications is being considered as a key feature for 6G [3].

Among the myriad of possible application scenarios, we have identified two that can benefit from RadCom, and that will be further examined in this contribution. The first one concerns networked automated traffic. Radar systems are already extensively employed in automotive systems, for instance in the 77-81 GHz spectrum [4], with highly directive antennas. These systems can be enhanced by including communications capability. For example, one car can identify an object on the road, like a pedestrian or an animal, and, at the same time, convey this information to an approaching vehicle, while coordinating their trajectories. Radar-enabled communications can also be employed between roadside infrastructure and vehicles, to assist them in the decision making. The second scenario concerns autonomous robots interacting with each other and with humans in the same environment, as in factory floors or in street delivery. In this scenario, it is essential that the robots can identify the presence of humans and other obstacles to avoid accidents or plan their movements. This scenario may involve high mobility and use communication at lower carrier frequencies and less directive antennas. These scenarios are depicted in Fig. 1. The field of possible applications that can make use of radar information is immense. As we move into higher frequencies, filling the THz gap [3], many applications beyond object detection can be envisaged, such as spectroscopy, for instance. Besides, environment awareness can also be useful to optimize the communications link itself, as we can identify obstacles to signal propagation or possible reflectors. As proposed in [5], the propagation information can be used to assist beam alignment and enhance the wireless link quality.

Our challenge in this work is to design a waveform that is suitable for both sensing and communications, and that can operate at a fast changing scenario with little or no central coordination. Some proposals in the literature require the use of full duplexing for joint sensing and communications, but this technique is still too expensive and power consuming. Therefore, we favour a waveform which works in half-duplexing and requires low-cost efficient hardware and signal processing. With these requirements in mind, we propose a chirp-based waveform, which is presented in Section II. Chirps have been extensively used in radar systems [4], and can also be modulated with little impact on the radar performance. Chirp-based modulation is employed, for instance, in LoRaWAN. Chirps can also be seen as a spread-spectrum system, which can cope with jamming or non-intentional interference.

Moreover, security and privacy are likely to be critical issues for the success of the future connected world. Indeed, sensing and communications applications are not an exception, as confidential information, such as user location and identity, may be conveyed through the communications link. Sensing also raises some privacy concerns, and the object detection should be employed only for the desired purposes, i.e., to increase safety, but not for tracking individuals without permission, for instance.

In this context, physical-layer security (PLS) is a promising technique that can help us to provide an additional layer of security to a RadCom system. Key-less coding PLS methods can guarantee perfect security [6], but rely on many assumptions about the capabilities of the eavesdroppers and the channel conditions, which are hard to guarantee in practice [7]. We argue that the extraction of encryption keys from a common random source [8], [9], such as the propagation channel is a more feasible proposal. As this depends on the intrinsic physical characteristics of the propagation channel, it facilitates the key exchange and distribution in highly dynamic scenarios, such as the ones presented here. For radar detection the signal should have a large bandwidth, and, thanks to the chirp waveform the spectrum is nearly flat over the whole bandwidth. Knowing that, we propose a filterbank-based PLS

This work is financed by the Saxon State government out of the State budget approved by the Saxon State Parliament.

technique, which is able to generate keys by decomposing the received signal in parallel sub-bands. This contributes to increase the key generation rate with respect to received-signal-strength-indicator (RSSI)-based methods found in the literature [10]. This is described in Section III.

Both RadCom and PLS are briefly analysed in the same context using the QuaDRiGa channel simulator [11] in Section IV. This new concept poses some challenges for the hardware implementation, and these are briefly discussed in Section V.

II. Joint sensing (radar) and communications

The frequency-time representation of the proposed chirp waveform in one frame is given in Fig. 1(c), where B_s, T_c represent the chirp-sequence sweep bandwidth and duration, respectively. The preamble consists of M_p non-overlapping unmodulated chirps, whereas the data part consists of M_c QAM-modulated overlapping chirps, spaced by Δt.

The j-th data chirp, denoted as $s_{c,j}(t)$, modulated with the message signal α_j at a carrier frequency f_c, is given as

$$s_{c,j}(t) = \Re\left\{\alpha_j \exp\left(\iota 2\pi \left(f_c - \frac{B_s}{2}\right) t + \iota\pi S t^2\right)\right\}, \quad (j-1)\Delta t < t \leq (j-1)\Delta t + T_c \tag{1}$$

where $S = \frac{B_s}{T_c}$ is the chirp slope and T_c is chosen as $T_c = 2D_o/c$, with D_o the radar operating range [12]. $\alpha_j, 1 \leq j \leq M_c$ is drawn from an M-ary complex constellation $\left\{\alpha^{(m)}\right\}, 1 \leq m \leq M$ and Δt the intersymbol interval. Existing spread-spectrum RadCom systems [1], [13], [14] consider $\Delta t = T_c$, resulting in a poor spectral efficiency. It can be demonstrated however that chirps can overlap and remain orthogonal only if $\sqrt{B_s T_c} \in \mathbb{Z}$ and

$$\Delta t = \sqrt{\frac{T_c}{B_s}}. \tag{2}$$

This increases the spectrum efficiency of the proposed system by a factor of $\sqrt{B_s T_c}$ in relation to existing spread-spectrum techniques. The data part of the frame is then given by $x_c(t) = \sum_{j=1}^{M_c} s_{c,j}(t)$, and, finally, we concatenate preambles and data. Next we present sensing and communication using the proposed waveform.

A. Sensing

Considering a single reflection from the target distance d, the noiseless signal at the radio frequency (RF) radar receiver front-end is

$$y_{rad}(t) = h_r x(t - t_d), \tag{3}$$

where h_r is the reflection attenuation, dependent on the radar cross section and distance of the target, and $t_d = 2d/c$ is the round-trip delay. We assume a slowly moving target, ignoring the effect of Doppler shift. The received signal (3) after mixing and filtering is simplified as

$$\underline{z}(t) = \begin{cases} \frac{1}{2} h_r \sum_{i=1}^{M_p} \cos\left(2\pi S t_d t\right), (i-1)T_c + t_d < t \leq iT_c \\ \frac{1}{2} h_r \sum_{i=1}^{M_p} \cos\left(2\pi \left(B_s - S t_d\right) t\right), \ iT_c < t \leq iT_c + t_d \end{cases}$$

The binary hypotheses testing problem to decide the absence $(\mathcal{H}_0)$ or presence $(\mathcal{H}_1)$ of the target is given as

$$\mathcal{H}_1 : z_{rad}(t) = \underline{z}(t) + w_{rad}(t); \ \mathcal{H}_0 : z_{rad}(t) = w_{rad}(t), \tag{4}$$

where $w_{rad}(t)$ is the radar receiver noise, which is assumed to be zero-mean Gaussian with variance σ^2_{rad}. Let $Z_{rad}[k]$ be the DFT of the sampled signal $z[n] = z_{rad}(kT_s)$, with T_s the sampling interval. Employing the conventional automotive radar receiver processing [12], [14]–[16], the K-point FFT-based detection statistic is given as

$$\mathcal{T} = \max_{k \in \{0,1,\ldots,K-1\}} Z_{rad}[k] \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma, \tag{5}$$

B. Communication

Let $\tilde{h}_c[n,l]$ denote the ν-tap communication channel discrete-time impulse response of the l-th frame, such that $0 \leq n \leq \nu - 1$. The channel is time correlated across frames due to the mobile application scenarios discussed in Fig. 1, and is modeled using QuaDRiGa channel simulator, discussed in detail in section IV. The discrete-time complex baseband received communication signal is

$$\tilde{y}_c[n,l] = \tilde{h}_c[n,l] \circledast \tilde{x}_c[n,l] + \tilde{w}_c[n,l], \ 0 \leq n \leq N_c, \tag{6}$$

where $\circledast$ denotes the convolution operation and N_c is the number of samples in the communications part of the frame, with duration $(M_c - 1)\Delta t + T_c$. $\tilde{x}_c[n,l]$ above is the transmitted baseband communication signal and $\tilde{w}_c[n,l]$ denotes the communication channel noise, assumed to be white zero-mean complex Gaussian with variance σ_c^2. The system model assumes perfect synchronization and knowledge of the channel state information at the receiver, which can be achieved using the preamble. Representing $\tilde{y}_c[n,l]$ as a column vector $\mathbf{y}_c[l] \in \mathbb{C}^{N_c \times 1}$, one obtains

$$\mathbf{y}_c[l] = \mathbf{H}_c[l]\mathbf{C}\mathbf{a}[l] + \mathbf{w}_c[l], \tag{7}$$

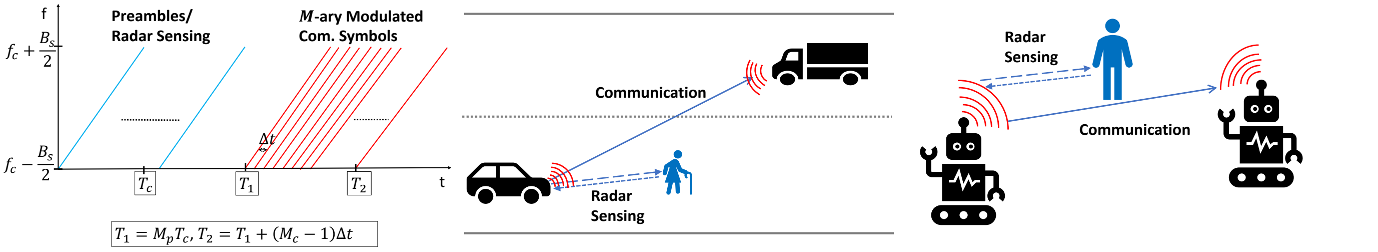
where $\mathbf{w}_c[l] \in \mathbb{C}^{N_c \times 1}$ is the noise vector, and $\mathbf{a}[l] = [a_1[l], a_2[l], \ldots, a_{M_c}[l]]^T$ denotes the complex modulated symbol vector. The matrix $\mathbf{C} \in \mathbb{C}^{N_c \times M_c}$ is the baseband chirp transform matrix with the j-th column vector $\mathbf{c}_j$ given as

$$\mathbf{c}_j = \left[\mathbf{0}^T_{(j-1)\Delta n}, \mathbf{c}^T, \mathbf{0}^T_{(M_c - j)\Delta n}\right]^T, \ 1 \leq j \leq M_c, \tag{8}$$

where $\mathbf{c} = \left[1, \exp\left[\iota\pi S T_s^2\right], \ldots, \exp\left[\iota\pi S (N-1)^2 T_s^2\right]\right]^T$ and $\Delta n = \Delta t / T_s$ with $N = \frac{T_c}{T_s}$ denoting the number of samples in a chirp duration. $\mathbf{H}_c[l] \in \mathbb{C}^{N_c \times N_c}$ is the lower-triangular frequency-selective channel matrix. Let $\mathbf{\Psi}[l] = \mathbf{H}_c[l]\mathbf{C}$, then the symbols can be estimated using an minimum mean-square error (MMSE) equalizer, as

$$\hat{\mathbf{a}}[l] = \left(\mathbf{\Psi}^H[l]\mathbf{\Psi}[l] + \sigma_c^2 \mathbf{I}\right)^{-1} \mathbf{\Psi}^H[l] \mathbf{y}_{com}[l], \tag{9}$$

which has complexity of the order of M_c^2, owing to the lower triangular structure of the matrix $\mathbf{\Psi}[l]$.



(a) (b) (c)

Fig. 1. (a) Frequency-time $(f - t)$ response of the transmitted signal $x(t)$ with M_p non-overlapping preambles and M_c overlapping communication symbols; (b) and (c), joint RadCom system scenarios: automotive and robotics.

III. Physical-Layer Security

According to the PLS concept, the chirp-based frames exchanged between the two communicating terminals can be reused for security purposes to generate encryption keys, in what we name here channel-reciprocity-key-generation (CRKG). In this regard, we propose a novel scheme based on a filterbank. We focus on a wideband approach that opens new opportunities for PLS key generation. In fact, the time and frequency diversity of the radio channel is deemed to be the common entropy source, from which the security keys are derived. Differently from RSSI-based methods [17], which provide approximately only tens of bits per second as key generation rate, the filterbank is theoretically capable to increase the bit generation rate up to thousands per second, with enough degrees of freedom to be adaptive to the channel conditions. By design, the proposed filterbank is envisioned to be an auxiliary component of the physical receiver architecture, but further investigations are necessary to explore if it could be capable to enhance the security of the RadCom system in a compatible way with upper protocol stack and existing cryptography schemes.

The goal of the filterbank is to obtain the channel reciprocity information through P filters, which capture the chaotic nature of the multipath in the frequency domain, as this is a unique signature between two communicating entities. The filterbank does not perform channel estimation exactly, but just measures the signal power at the output of each p-th filter. Because of the flat power spectrum of the transmitted chirp signal, the filters output is therefore a direct function of the channel impulse response.

The filterbank input is the received communications signal $\tilde{y}_c$, which contains the communication data, the channel dispersion and the noise. Then, the output of the p-th filter is given as

$$O_p = \int_{\Delta_{fp}} F_p(f) \cdot |\mathcal{F}[\tilde{y}_c](f)|^2 \, df, \ \forall p \in [1, P], \qquad (10)$$

where Δ_{fp} and $F_p(f)$ are, respectively, the bandwidth and the filter frequency response of the p-th filter; whereas the $\mathcal{F}[\tilde{y}_c]$ is the Fourier transform of the filterbank input $\tilde{y}_c$. $F_p(f)$ is modelled as an ideal band-pass finite-impulse-response filter with a sub-bandwidth $\Delta_{fp} = B_s/P$. Then, each filterbank output coefficient O_p is quantized into bits, for example, with two thresholds and a censor zone in between [8]. In details, the p-th thresholds determining 1s and 0s bits in the security key are set respectively adding a positive and negative margins to the median value of the collected O_p [9]. This is computed for each filterbank output and for each processed frame. The quantization levels have been optimized with a trial-and-error procedure, in order to empirically achieve the minimum number of mismatched bits in the keys. The same filterbank settings with $P = 128$ are consistently used throughout all the simulations, . Further optimizations are left out and will be included in future works. With regard of the complete PLS CRKG protocol, no reconciliation nor amplification protocols have been applied on the *raw* extracted key. These protocols are out of the scope of this work.

Finally, it is worth reminding that the proposed filterbank-based is a general CRKG purpose solution, capable to work with any waveform and radio channel conditions, as long as the transmit power spectrum density is known.

IV. Simulation Results

This section presents a performance analysis of the proposed RadCom system for the application scenarios in Fig. 1. The communication channel impulse response is simulated using QuaDRiGa channel simulator [11]. QuaDRiGa is a fully-fledged three-dimensional geometry-based stochastic channel model compliant with 3GPP specifications with many noticeable features: spatial consistency, multi-frequency simulations and dual mobility. As shown in Fig. 1(a),(b) both terminals are equipped with a single transmit/ receive antenna. The system parameters are specified in Table I. On the other hand, the radar channel consists of a single stationary target present at a distance of $d = 15$ m in front of the moving terminal.

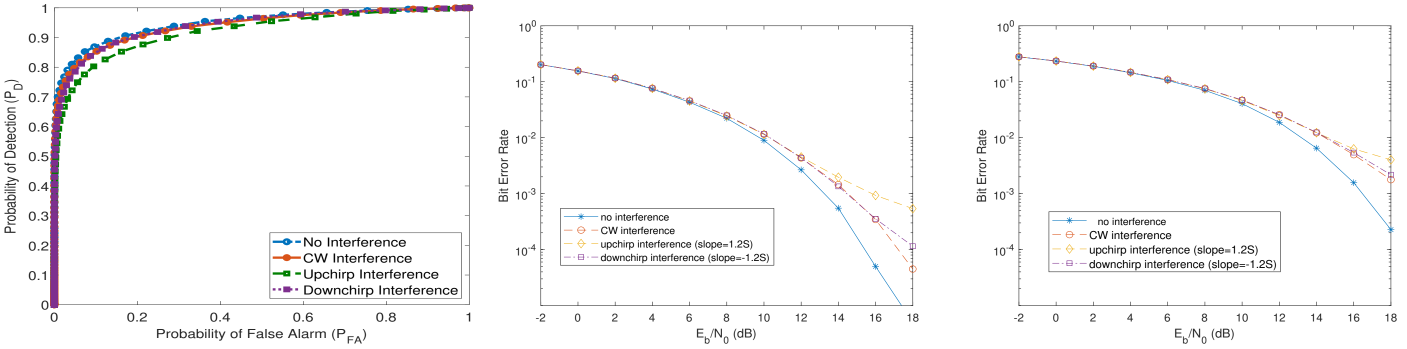
TABLE I
Numerical simulations parameters

Parameter	Automotive	Robot
carrier	78 GHz	3.7 GHz
bandwidth	1 GHz	80 MHz
speed	35 m/s	8 m/s
antenna	directive	dipole-like
scenario	highway	industrial
track length	100 m	100 m

A. *Sensing & Communication Performance*

The sensing and communication performances of the proposed system are analysed for both application scenarios, with and without interference, as described in the following.

In this context, we consider either a narrowband phase-modulated continuous wave (CW) interference acting as a



(a) (b) (c)

Fig. 2. RadCom system with and without CW, upchirp, downchirp interferences: (a) Radar sensing performance ($d = 15$m, 3 preambles and SIR $= -5$dB); (b) BER versus E_b/No in the automotive scenario and (c) in the robotics scenario (16-QAM overlapping chirp, SIR $= 10$dB)

jammer at a frequency of $f_c + 0.4$ GHz, or wideband phase-modulated upchirp/downchirp interferers occupying the same frequency bands with slope $1.2S$. The chirp duration is set as $T_c = 1.024$ μs with sweep bandwidth $B_s = 1$ GHz, 80 MHz for the automotive and robotic scenarios, respectively. A single frame consists of $M_p = 3$ preambles and $M_c = 100$ communication symbols modulated using M-ary quadrature amplitude modulation (QAM) with $\Delta t = 32$ ns, 113.1 ns.

Fig. 2(a) presents the radar sensing performance simulated using non-overlapping chirp preambles in terms of detection and false-alarm probabilities P_D, P_{FA}. The radar signal-to-noise ratio (SNR) is -24 dB and signal-to-interference ratio (SIR) is -5 dB. It can be seen that for a given P_{FA}, the detection probabilities with a CW interferer and with an opposite-slope chirp interferer are fairly close to that without interference. The robustness of the proposed system against a CW narrowband interferer occurs due to the spread-spectrum characteristics of the proposed system. In case of an interfering chirp, the cross-correlation between the desired signal and the interferer decreases with an increasing difference between the slopes. Thus, with a slope in the opposite direction, we observe a low correlation and little interference. On the other hand, an upchirp interferer with an absolute slope difference of 0.2 leads to a higher correlation between the two wideband systems, thereby degrading the system performance. The radar channel is the same for both scenarios.

Moreover, the communication performance is analyzed in terms of bit error rate (BER) curves as shown in Fig. 2(b), Fig. 2(c) for both the channel models, automotive and robotic, in Fig. 1(a), Fig. 1(b), considering SIR $= 10$ dB, where the interferer does nor suffer any fading. It can be seen that the system is quite robust against interference, especially in the presence of an CW interferer or of a chirp interferer with opposite slope. We can see that BER increases with an upchirp interferer, which has a lower slope difference.

B. Security Keys Performance

The results of the PLS CRKG for the two scenarios are presented in Fig. 3. The performances are given in terms of percentage of mismatched bits (left axis and blue color), and in terms of minimum entropy (right axis and red color). These are obtained averaging over all the snapshots along the scenarios route, in order to test the CRKG for each frame exchanged. The agreement error can be considered the biggest hurdle for CRKG reliability, because any disagreement between the two terminals might lead to a complete failure of the CRKG process. The main causes are caused here given by AWGN noise and time-division-duplex (TDD) delay (i.e. round-trip-time). In this work, we focus on the assessment of the reciprocity of the key generation, neglecting any analysis about malicious eavesdropper. Thus, the goal is to show the feasibility of PLS CRKG thanks to the chirp-waveform properties.

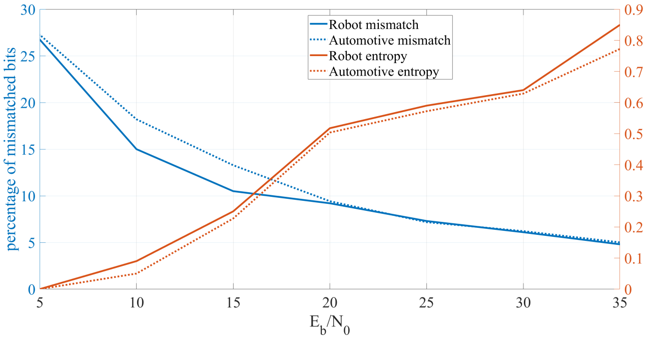


Fig. 3. Percentage of mismatched bits in the generated keys (left axis) and minimum entropy of the generate key (right axis).

It is hard to perform a direct comparison between the two scenarios, since antennas, carrier and bandwidth are different, resulting in different QuaDRiGa channel coefficients. However, the two simulated scenarios, automotive and robots, show similar PLS results, as it can be seen in Fig. 3. The vehicular scenario (dotted lines in figure) is slightly worse than the robot scenario (solid lines in figure), mainly because of the higher speed. PLS works better in a high-SNR regime, as expected. For example, starting from 15dB of E_b/N_0, the CRKG provides a key-error percentage lower than 10%, and a minimum entropy larger than 0.3, approximately. The issue of mismatching bits can be fixed by utilizing a reconciliation protocol after quantization, for example using forward-error-correcting codes. On the other hand, in the lower Eb/N_0 region, the PLS results become poorer, because of the non-reciprocal noise processes at the communication ends. Not only more errors in the keys occur because of the different filterbank outputs coefficients, but also there exists a biased generation of 1s rather than 0s. This directly reduces the quality of the generated key, i.e. lower entropy. This result is due to the set-up of the filterbank, tuned to reduce the mismatching conditions, rather than to obtain a uniform key. This is a common CRKG trade-off. However, the imperfection in the randomness of the raw key can fixed (after a reconciliation protocol) with a privacy amplification method, for example using a hash function. In all simulation runs, the number of censored bits between the quantization thresholds is less than 80%. This leads to a minimum of approximately 100 bits of security keys per frame exchange.

V. Hardware challenges

For a RadCom system, the main hardware challenges come from the different requirements of linearity, mixer operation and the operation of the combined transmitter. There are three radio-frequency (RF) components in such a system: the combined transmitter, the radar receiver and the communication receiver. The combined transmitter should meet all the communication system specification, while maintaining the bandwidth requirements of the wideband radar signal. The radar receiver complexity depends heavily on the waveform used. For a non-overlapping linear chirp waveform [12], the receiver operation is fairly simple and can have little power consumption by designing a wide band mixer that multiplies the transmit signal and the received signal (reflected from the objects). However, when the waveform used is not a chirp waveform, the radar receiver power consumption and complexity can be similar to the communication receiver with some leverage for linearity, noise and interference due to relaxed auto-correlation requirements. In the joint system, we achieve the operation with one antenna operating in TDD mode between combined transmitter and communication receiver whereas the second antenna is needed for the radar operation. However, these two antennas should have enough isolation to reduce the direct interference and the RF circuits should have on-chip isolation as well. That is why the leakage of local oscillation and power amplifier to the radar receiver mixer is particularly important for extracting timing information apart from the isolation between these two antennas. The primary challenge for the communication receiver is to meet both the bandwidth and linearity requirements, as high resolution radars using linear chirps will require higher bandwidth as well.

From security point of view, the physical layer security principle relies heavily on the fact that the radio channel is reciprocal. Unfortunately, the communication channel, including the RF chain might be non-reciprocal. Ideally, the combined (i.e. Tx and Rx) RF chain performance (between the two terminals) are reciprocal and do not vary over time. Given the antennas are mostly used in TDD mode, the primary hardware challenges are to maintain the wide-band linear amplification in the RF chain and to conduct an accurate initial calibration of the transceiver chain, to be able to compensate or reduce the non-reciprocal impairments.

VI. Conclusions and further Work

In this contribution we have presented a novel chirp-based waveform that can be employed efficiently for both communications and radar sensing. This technologies convergence is likely to be a key 6G feature, allowing low-complexity and convenient hardware solutions. Using realistic channel models for both automotive and robotics applications, we have shown that chirp modulation is robust against jamming and interference, and, additionally, is suitable for generating encryption keys from the reciprocal channel, by means of a new filterbank processing method.

Leveraging on these promising preliminary results, we will perform further studies in communication, radar and security domains. These include a system-level analysis, a more detailed channel model for the radar detection and an optimization of the filterbank parameters to improve the key generation entropy and agreement rate.

References

[1] C. Sturm and W. Wiesbeck, "Waveform design and signal processing aspects for fusion of wireless communications and radar sensing," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1236–1259, 2011.

[2] B. Paul, A. Chiriyath, and D. Bliss, "Survey of RF communications and sensing convergence research," *IEEE Access*, vol. 5, pp. 252–270, 2017.

[3] K. L. Matti Latva-aho, "Key drivers and research challenges for 6G ubiquitous wireless intelligence," 6G Flagship, Tech. Rep., 2019.

[4] J. Hasch *et al.*, "Millimeter-wave technology for automotive radar sensors in the 77 GHz frequency band," *IEEE Transactions on Microwave Theory and Techniques*, vol. 60, no. 3 PART 2, pp. 845–860, 2012.

[5] N. González-Prelcic, R. Méndez-Rial, and R. W. Heath, "Radar aided beam alignment in mmWave V2I communications supporting antenna diversity," in *2016 Inform. Theory and Applic. Workshop (ITA)*, Jan 2016.

[6] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[7] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[8] S. Mathur *et al.*, "Radio-telepathy," in *Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom '08*. New York, New York, USA: ACM Press, 2008, pp. 128–128.

[9] J. Zhang *et al.*, "Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview," *Entropy*, vol. 19, no. 8, pp. 420–420, Aug. 2017.

[10] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, August 2011.

[11] Fraunhofer-HHI, "QUAsi Deterministic RadIo channel GenerAtor," https://quadriga-channel-model.de, 2019.

[12] S. M. Patole *et al.*, "Automotive radars: A review of signal processing techniques," *IEEE Signal Proc. Mag.*, vol. 34, no. 2, pp. 22–35, 2017.

[13] S. Dokhanchi *et al.*, "Multicarrier phase modulated continuous waveform for automotive joint radar-communication system," in *International Workshop on Signal Process. Advances in Wireless Comm.* IEEE, 2018.

[14] S. Dwivedi *et al.*, "Target detection in joint frequency modulated continuous wave (FMCW) radar-communication system," in *International Symposium on Wireless Comm. Systems*. IEEE, 2019.

[15] F. Ahmed, K. Elbarbary, and A. Elbardawiny, "Analytical performance evaluation of an enhanced frequency domain radar detector," in *Radar Conf.* IEEE, 2008.

[16] S. Neemat, O. Krasnov, and A. Yarovoy, "Simultaneous processing of time-shifted orthogonal LFMCW waveforms," in *Signal Process. Symposium*. IEEE, 2017.

[17] J. Wan, A. B. Lopez, and M. A. Al Faruque, "Exploiting Wireless Channel Randomness to Generate Keys for Automotive Cyber-Physical System Security," in *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, Apr. 2016, pp. 1–10.