Spatio-temporal modulated mm-Wave arrays for physical layer security and resiliency against distributed eavesdropper attacks

Suresh Venkatesh
suresh.venkatesh@princeton.edu
Princeton University
Princeton, New Jersey, USA

Xuyang Lu
xuyang.lu@sjtu.edu.cn
UM-SJTU Joint Institute
Shanghai, China

Kaushik Sengupta
kaushiks@princeton.edu
Princeton University
Princeton, New Jersey, USA

ABSTRACT

Ensuring security for the next-generation of millimeter-Wave and Terahertz networks, while simultaneously ensuring multi-Gbps data rates and ultra-low latency (sub-millisecond) is becoming increasingly challenging. Physical layer security that exploits the physics of wireless propagation to incorporate security features into the signal is becoming increasingly popular as a component for a holistic approach towards ensuring security. In this regard, there are prior works that have exposed severe vulnerabilities in the well-established principle of security that involve directional narrow beams. In this article we highlight security features using mm-Wave interface design, and present a generalized approach towards physical-layer security. Security in our approach is ensured by enforcing fundamental loss of information by selective spectral aliasing towards the direction of eavesdroppers while maintaining robust, high fidelity wireless link towards the intended receiver. In a custom-designed integrated transmitter array, spectral aliasing is achieved by dynamically reconfigurable symbol-to-antenna mapping principle that can synthesize a fast time-varying channel towards the direction of the eavesdroppers. We demonstrate this principle experimentally for the first time with mm-Wave directional links (71-76 GHz unlicensed spectrum). We also experimentally show the resilience of such links against distributed and synchronized eavesdropper attacks for the first time in the mm-Wave bands.

CCS CONCEPTS

• **Hardware** → Integrated circuits; Wireless devices; • **Security and privacy** → Hardware security implementation.

KEYWORDS

millimeter-wave, arrays, physical-layer security, eavesdropper, distributed attack, spatio-temporal modulation, machine learning.

ACM Reference Format:

Suresh Venkatesh, Xuyang Lu, and Kaushik Sengupta. 2022. Spatio-temporal modulated mm-Wave arrays for physical layer security and resiliency against distributed eavesdropper attacks. In *5th ACM Workshop on Millimeter-Wave and Terahertz Networks and Sensing Systems (mmNets '21)*, January 31–February 4, 2022, New Orleans, LA, USA. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3477081.3481673>

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

mmNets '21, January 31–February 4, 2022, New Orleans, LA, USA

© 2022 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-8699-9/22/01.

<https://doi.org/10.1145/3477081.3481673>

Figure 1: Wyner wire-tap models a. A conventional channel capacity (SNR) differential towards to achieving security. b. An approach towards physical layer security through spatio-temporal modulation that enforces intentional spectral aliasing towards the eavesdropper direction, while maintaining a high-fidelity channel towards the intended receiver through emulation of a time-varying side channel [20].

1 INTRODUCTION

Cyber physical security is emerging as one of the central challenges in the ongoing transformation of wireless networks and connectivity. This is particularly exacerbated as a new spectral range in the millimeter-Wave frequencies becomes available to us creating a spectral span that is several orders of magnitude larger than we ever have had access to [5, 9–11, 14, 15, 17, 19, 22]. In this new wireless paradigm, ensuring security at ultra-high speed data rates (multi-Gbps) and ultra-low latency (sub-millisecond) is becoming increasingly challenging. A more holistic approach to security that encompasses physical layer security techniques can overcome some of these challenges, and is being actively explored as we prepare for security for networks in 5G and beyond [1–4, 8, 18, 24]. The process relies on utilizing the physics of signal propagation to incorporate security features without an explicit key exchange. However, prior

Figure 2: Concept of spatio-temporal modulated arrays. a. A traditional phased array where spectrum and constellation remains preserved in space. **b.** A spatio-temporal modulated array operation with symbol-to-antenna mapping in a time-modulated fashion. **c.** Comparison of bit-error-rate as a function of elevation angle for a 4-element phased array and 4-element spatio-temporal modulated array. **d.** Measured variation of the spectral aliasing and secure cone as a function of modulation frequency, f_{mod} for a data bandwidth of 200 MHz QPSK signal at $f_c = 76$ GHz. Secure cone is established for $f_{\text{mod}} < \text{signal bandwidth}$ [6, 20]. **e.** Custom designed 71-76 GHz 4-element with CMOS spatio-temporal modulated array (STMA) chips and packaged antennas [6], demonstrating the EM co-design approach. Each chip integrates a 2-element STMA.

works have demonstrated that in spite of enhanced security due to directional beams, wireless mm-Wave/THz links are still vulnerable to eavesdropping [7]. New physical layer techniques are needed to address the security needs of this unique spectrum [12, 13, 16]. Here, we combine security features in the mm-Wave interface design itself, and demonstrate a generalized physical-layer security approach where secrecy is imparted by enforcing fundamental loss of information through intentional and selective spectral aliasing towards the directions of the eavesdroppers.

In this article, we achieve physical layer security by emulating a fast time-varying channel towards the direction of eavesdroppers even though the channel can be physically static. We presented the findings in [6, 20], and here we highlight the importance of a co-design of the integrated reconfigurable spatio-temporal modulated arrays on the physical layer security for future wireless communication. We show how such physical layer security can be achieved with a unique and dynamically reconfigurable symbol-to-antenna mapping methodology, and we demonstrate such physical layer security techniques for the first time in the mm-Wave regime with custom designed silicon chipsets operating in the 71-76 GHz unlicensed spectrum (Fig. 2e). We show how narrow and dynamically reconfigurable secure wireless zones can be established with the presented method, and also present techniques to obfuscate distributed and synchronized eavesdropper attacks [6]. We demonstrate analytically and experimentally resilience of such links against distributed and colluding eavesdropper attacks (including those based on channel inversion and machine-learning based neural network model) for the first time in these frequency ranges [20]. The wireless transformation through 5G (and future 6G and beyond) is expected to

have a tremendous impact on communication systems and technologies in the near future.

2 PHYSICAL LAYER SECURITY: CONCEPT OF SPATIO-TEMPORAL MODULATED ARRAYS

A physical layer security approach relies on having different gain channels between the transmitter (Alice) and the intended receiver (Bob) compared to the channel gain between the transmitter and the eavesdropper (Eve) (Fig. 1 (a)). Given the channel gain for Alice-Bob is h_B and Alice-Eve is h_E , and the noise variance at Alice is σ_B^2 and σ_E^2 , the secrecy capacity is given by the difference between the channel capacities [8]

$$C_s = \frac{1}{2} \log \left(1 + \frac{P|h_B|^2}{\sigma_B^2} \right) - \frac{1}{2} \log \left(1 + \frac{P|h_E|^2}{\sigma_E^2} \right) \quad (1)$$

A directional beam established by phased arrays naturally incorporates this security by reducing the signal leakage to other angles [23]. However, in a conventional phased array, the same symbol series are fed into all the antennas in the array along with appropriate phasing to direct the beam towards the intended receiver. This results in the signal constellation and spectrum to be preserved across all other angles, albeit with lower SNR (Fig. 1). This makes the channel vulnerable to a potential eavesdropper attack with a sensitive receiver located at any of the sidelobes. Such a security approach based on SNR differential is illustrated in Fig. 1 (a) and the corresponding phased array is illustrated in Fig. 2 (a).

A spatio-temporal array approach, on the other hand, attempts to impart physical layer security, by intentionally introducing spectral aliasing along the channel path to the eavesdropper while still

Figure 3: Measurement of QPSK Constellation (IF data bandwidth = 200 MHz) and received spectrum across all spatial elevation angles (at carrier frequency of 76 GHz). a. Measurements for a conventional 2-element phased array showign preservation of signal spectrum and constellation in space. b. Measurement for a spatio-temporal modulated array with a periodic switching frequency $f_{\text{mod}} = 0.5 \times \text{IF Bandwidth}$, demonstrating preservation of signal spectrum and constellation at the broadside while spectrally aliasing at other angles. c). Measured security cone for different f_{mod} , the switching frequencies and a given signal bandwidth of 200 MHz [20].

maintaining a high fidelity link to the intended receiver. A concept model is illustrated in Fig. 1 (b), where spectral aliasing and constellation scrambling is enforced away from the intended direction through emulation of a time-varying side channel.

In a spatio-temporal modulated array (STMA) (Fig. 2), the symbols (or fractions of them) are mapped into antennas (or subsets of them) in a time-modulated fashion. The figure shows a simple example, where the series of symbols are chopped off in such a fashion that each symbol is mapped into a separate antenna. As a result, with equal phase settings ($\Delta_l = 0^\circ$), all the symbols align in time only at the broadside to recreate the original signal, while creating severe symbol mis-alignment in any other directions. From a spectral perspective it can be seen that the mapping of the symbol-to-antenna (time-modulation) creates spectral aliasing at each antenna. At the direction of interest (broadside in this example), the aliased components cancel to create a high fidelity link to Bob, while retaining the spectral aliasing at all other directions rendering the desired physical layer security (Fig. 2 (b)). The comparison of bit-error-rate (BER) as a function of spatial angle for a 4-element phased array and an STMA is shown in Fig. 2 (c). As can be understood, secure cone is established when the modulation frequency ($f_{\text{mod}} < \text{BW}$) is less than the bandwidth of the signal. With custom designed silicon chips and integrated signal processing as we show here, one can enable more complex mapping that creates non-repetitive rotations of the constellations at the eavesdroppers. As an example, the mapping can be time-varying with frequency chirps or each symbol can be divided into irrational fractions and mapped to multiple antennas. In a spatio-temporal modulated system, it is important to note that the security metric enhancement factor (BER level at the first side-lobe level) is related with number of elements in the phased array, sub-array size (number of elements collectively transmitting at a given time instant), type of time modulation. Depending on the number of sub-array size the requirement on the transmitter power per element can also be derived to meet the link budget.

3 SPATIO-TEMPORAL MODULATED ARRAY MEASUREMENTS AND ANALYSIS

The demonstration of a generalized physical layer security and establishment of secure wireless zones in space is achieved through custom-designed silicon chipsets operating as 2-element and 4-element array in the mm-Wave band across 71-76 GHz [6]. The presented methodology can potentially be scalable to larger arrays allowing for dynamic establishment of secure zones in space. All the measurements shown in Fig. 3 and Fig. 4 correspond to a two-element array. The silicon chipset realized on an industry standard CMOS platform consists of two independently controllable transmitter chain. Each transmitter chain has a capability to output +9 dBm of power which is then radiated out with packaged series-fed patch antennas (Fig. 2e) [21]. This requires a careful EM co-design approach between the integrated chip and the packaged antenna to achieve both time modulated and high efficiency output power.

When the time modulation signal is turned off, the two elements behave as a conventional phased array. At $\theta = 0^\circ$, the wireless link is established (Alice-to-Bob) and the spectral power is high with good SNR (main lobe) for a QPSK link. This spectrum can be demodulated and the recovered constellation is shown in Fig. 3(a). As we increase the spatial angle away from from the intended receiver, the spectral power reduces in accordance with the angular beam pattern, while still preserving the spectrum and the constellation, as can be seen in Fig. 3 (a).

Figure. 3(b) demonstrates the measurements of the same link with a spatio-temporal modulation operation, when the symbols are modulated with frequencies less than the bandwidth of the signals. In this case, the time modulation signal is chosen to be $f_{\text{mod}} = 100 \text{ MHz}$, where the signal IF bandwidth is 200 MHz. This implies that in the symbol-to-antenna mapping, every alternate symbol is transferred to the other antenna. As can be seen, the broadside the link between Alice-to-Bob (intended receiver) is well established by cancelling all the aliased spectral

Figure 4: Chirped frequency switching for robust security. a. Measurement of QPSK Constellation (IF bandwidth = 200 MHz) and received spectrum across all spatial elevation angles (at $f_c = 76$ GHz) for different linearly chirped switching bandwidths. This creates a time-varying non-repetitive symbol-to-antenna mapping which is eventually shown as a countermeasure for a distributed eavesdropper attack. b. Effect on security cone angle for different chirped frequency bandwidths [20].

components. At angles away from the intended direction, the spectral aliasing and constellation garbling can be clearly seen. For both the cases, spectrum and constellation maps as a function of all elevation angles are shown in Fig. 3. The security zone establishment for different switching frequency is shown in Fig. 3 (c). With chirp modulated switching, there are two effects that are responsible for the creation of secure zones. Firstly, frequencies below the data bandwidth (BW), ($f_{mod} < BW$) lead to aliasing of the data BW and frequencies above the data BW lead to harmonics of the data BW and create noise like spectrum at the receiver as shown in Fig. 4a (for $\theta = 60^\circ$).

More complex time-modulations can have interesting security features that can make breaking into the channel more challenging even for multiple colluding eavesdroppers, as we will show later. A time-varying symbol-to-antenna mapping established with a chirp signal can affect the constellation dynamics drastically, making it harder for an eavesdropper to learn the channel. In Fig. 4, we show a case where the switching frequency (f_{mod}) is chirped between the frequency values of 100 MHz to 800 MHz with a given IF data

bandwidth of 200 MHz. As can be seen in the measurements, while the main beam constellation and spectrum are well preserved, the off-angle spectrum is spread like noise raising the noise floor and even potentially jamming an eavesdropper. The measurements corresponding to this case are shown in Fig. 4 (a). The achieved security zones for different chirp frequency bandwidths are shown Fig. 4 (b).

4 COORDINATED DISTRIBUTED ATTACKS AND MITIGATION STRATEGIES

Here, we demonstrate for the first time experimentally distributed coordinated and synchronized attacks with multiple eavesdroppers, their strategies, limits and methods to mitigate these attacks. We perform the algorithms in two ways 1) Channel-inversion attacks: Assuming that the eavesdroppers know the channel, and 2) AI-based: Assuming the eavesdroppers do not know the channel, but has ability to learn from the control signals. In the following sections, we show that both approaches are resilient to multiple coordinated eavesdropper attacks and our approach doesn't need to have any apriori knowledge of the eavesdropper locations. Other approaches like RF jamming use a simple power approach to mitigate eavesdropper attacks which are extremely power hungry. Here we use the physics of wave propagation through spatio-temporal modulation to enable the same while maintaining a high fidelity link with the intended receiver without the need for any cryptographic key exchanges.

4.1 Channel Inversion based Attack

A channel inversion based attack can be mathematically formulated as follows (also shown in Fig. 5 (a)),

$$\mathbf{y}_{Eve} = \mathbf{H}_{A-E} \mathbf{x}_{Alice} + \mathbf{v} \quad (2)$$

where $\mathbf{y}_{Eve}$ is the received signal vector from multiple eavesdroppers, $\mathbf{H}_{A-E}$ is the channel matrix between the transmitter and the eavesdroppers (Alice- to-Eve), $\mathbf{x}_{Alice}$ is the transmitter excitation (Alice), and $\mathbf{v}$ is the associated noise vector. Therefore, in principle, a large array of eavesdroppers each receiving spectrally aliased signals, can potentially extract $\mathbf{x}_{Alice}$ and therefore find the information at Bob $\mathbf{H}_{A-B}\mathbf{x}_{Alice}$ with apriori knowledge of the channel matrix. However, this is very sensitive to the actual positions of the eavesdroppers and the accuracy of the known channel matrix. Shown in Fig. 5 (b) is an example of reconstruction of the original signal with measured spectrally aliased signals at three representative eavesdropper positions, demonstrating instance of a successful attack and a failed attack (that is dependent on eavesdropper locations) [20].

This approach is also highly sensitive to channel matrix errors. As shown in Fig. 5 (c), a slight error in the knowledge of the channel matrix can completely overwhelm the attack requiring an enormously large number of synchronized eavesdroppers making this attack impractical. We also present a countermeasure in terms of statistical measurements for a 2-element STMA using chirped frequency switching. Chirping the switching frequency leads to time-varying constellation dynamics and the recovery based on channel inversion is extremely hard. These measurements are shown in Fig. 5 (d).

Figure 5: A channel inversion approach for coordinated distributed attack. a. Model for a channel inversion attack, where the eavesdroppers are aware of the Alice-to-Eve and the Alice-to-Bob channel. **b.** The approach shows measured spectrally aliased signal at three representative eavesdropper locations, and measured reconstructed constellation for an instance of a successful attack and a failed attack (that is dependent on eavesdropper locations), thus illustrating the dependence on the determination of the channel matrix. **c.** Vulnerability of the channel inversion attack to errors in channel estimation for a 16-element simulated STMA. **d.** Statistical measurement of attacks with different distributed eavesdroppers locations for the 2-element STMA at 76 GHz on a 200 MHz QPSK signal. A frequency chirped switching outperforms in terms of robustness against colluding eavesdropper attacks compared to a periodic switching case [20].

4.2 AI-based Attack

Determination of the channel matrix is critical to the previous approach. However, without the knowledge of the channel matrix, an attack scenario can happen through understanding of the spatial constellation dynamics at different angles (eavesdropper locations) and training a neural network based on expected pilot bits. The conceptual figure of the neural network based attack is shown in Fig. 6 (a). We also measure and compare the two attack strategies for a 4-element STMA and is shown in Fig. 6 (b). As shown, the AI-based attack can overcome some of the shortcomings of the deterministic channel inversion method. We also perform statistical measurement of attacks with different distributed eavesdroppers locations for the 2-element STMA at 76 GHz on a 200 MHz QPSK signal and are shown in Fig. 6 (c). As can be seen, a frequency chirped modulation can spread the signal and raise the noise floor, outperforming its capability to mitigate colluding eavesdropper attacks compared to antenna subset switching, and hence could be used as a mitigation strategy against such attacks.

5 CONCLUSION

Here, we describe a generalized approach towards physical layer security using spatio-temporal-modulation techniques for directional mm-Wave links. We demonstrate such security features for the first time at mm-Wave frequencies using custom designed chipsets at 71-76 GHz. We discuss the trade-offs of modulation schemes from conventional subset switching to sub-symbol chopping at irrational fractions, and time-varying modulation. We also propose and experimentally verify two attack strategies and show the resiliency of the spatio-temporal modulated architecture against such attacks. We also provide a countermeasure to such colluding eavesdropper attacks through frequency chirped switching methods. Our approach is also scalable and the demonstrated methodologies can have broad implications on heterogeneous 5G networks that are resilient to distributed attacks.

Figure 6: AI-based attack. a. A neural network-based distributed attack, where the eavesdroppers do not have apriori knowledge of the channel and attempts to learn it through the measured garbled constellations. b. Measured average BER with different number of eavesdroppers for a 4-element STMA. Machine learning based attack outperforms channel inversion method since there is no requirement for the determination of the channel matrix. c. Statistical measurement of attacks with distributed eavesdroppers for the 2-element STMA at 76 GHz on a 200 MHz QPSK signal. A frequency chirped switching outperforms in terms of robustness against colluding eavesdropper attacks compared to a periodic switching case [20].

ACKNOWLEDGMENTS

The authors would like to thank AFOSR, ONR, and DARPA for the funding support.

REFERENCES

- [1] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen. 2016. A survey on multiple-antenna techniques for physical layer security. *IEEE Communications Surveys & Tutorials* 19, 2 (2016), 1027–1053.
- [2] Shuping Dang, Osama Amin, Basem Shihada, and Mohamed-Slim Alouini. 2020. What should 6G be? *Nature Electronics* 3, 1 (2020), 20–29.
- [3] J.M. Hamamreh, H.M. Furqan, and H. Arslan. 2018. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 21, 2 (2018), 1773–1828.
- [4] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing. 2017. Jamming strategies for physical layer security. *IEEE Wireless Communications* 25, 1 (2017), 148–153.
- [5] X. Lu, S. Venkatesh, and H. Saeidi. 2021. A review on applications of integrated terahertz systems. *China Communications* 18, 5 (2021), 175–201.
- [6] Xuyang Lu, Suresh Venkatesh, Bingjun Tang, and Kaushik Sengupta. 2020. Space-Time Modulated 71-to-76 GHz mm-Wave Transmitter Array for Physically Secure Directional Wireless Links. In *IEEE Intl. Solid-State Cir. Conf.* 86–88.
- [7] Jianjun Ma, Rabi Shrestha, Jacob Adelberg, Chia-Yi Yeh, Zahed Hossain, Edward Knightly, Josep Miquel Jornet, and Daniel M Mittleman. 2018. Security and eavesdropping in terahertz wireless links. *Nature* 563, 7729 (2018), 89–93.
- [8] H Vincent Poor and Rafael F Schaefer. 2017. Wireless physical layer security. *Proceedings of the National Academy of Sciences* 114, 1 (2017), 19–26.
- [9] T.S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G.N. Wong, J.K. Schulz, M. Samimi, and F. Gutierrez. 2013. Millimeter wave mobile communications for 5G cellular: It will work! *IEEE Access* 1 (2013), 335–349.
- [10] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhatib, and G. C. Trichopoulos. 2019. Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond. *IEEE Access* 7 (2019), 78729–78757.
- [11] W. Roh, J. Seol, J. Park, B. Lee, J. Lee, Y. Kim, J. Cho, K. Cheun, and F. Aryanfar. 2014. Millimeter-wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results. *IEEE Comm. Mag.* 52, 2 (2014), 106–113.
- [12] H. Saeidi, S. Venkatesh, C.R. Chappidi, T. Sharma, C. Zhu, and K. Sengupta. 2020. A 4x4 Distributed Multi-Layer Oscillator Network for Harmonic Injection and THz Beamforming with 14dBm EIRP at 416GHz in a Lensless 65nm CMOS IC. *International Solid State Circuits Conf.* (2020).
- [13] H. Saeidi, S. Venkatesh, X. Lu, and K. Sengupta. 2021. 22.1 THz Prism: One-Shot Simultaneous Multi-Node Angular Localization Using Spectrum-to-Space Mapping with 360-to-400GHz Broadband Transceiver and Dual-Port Integrated Leaky-Wave Antennas. In *2021 IEEE International Solid-State Circuits Conference (ISSCC)*, Vol. 64. 314–316.
- [14] K. Sengupta. 2019. Integrated circuits for terahertz communication beyond 100 GHz: Are we there yet?. In *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 1–6.
- [15] Kaushik Sengupta and Ali Hajimiri. 2016. Designing optimal surface currents for efficient on-chip mm-wave radiators with active circuitry. *IEEE Transactions on Microwave Theory and Techniques* 64, 7 (2016), 1976–1988.
- [16] Kaushik Sengupta, Xuyang Lu, Suresh Venkatesh, and Bingjun Tang. 2020. Physically Secure Sub-THz Wireless Links. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 1–7.
- [17] K. Sengupta, T. Nagatsuma, and D.M. Mittleman. 2018. Terahertz integrated electronic and hybrid electronic–photonic systems. *Nature Electronics* 1, 12 (2018), 622–635.
- [18] Y. Shiu, S.Y. Chang, H. Wu, S.C. Huang, and H. Chen. 2011. Physical layer security in wireless networks: A tutorial. *IEEE Wireless Communications* 18, 2 (2011), 66–74.
- [19] S. Venkatesh, X. Lu, H. Saeidi, and K. Sengupta. 2020. A high-speed programmable and scalable terahertz holographic metasurface based on tiled CMOS chips. *Nature Electronics* (2020), 1–9.
- [20] Suresh Venkatesh, Xuyang Lu, Hooman Saeidi, and Kaushik Sengupta. 2021. Secure Millimeter-Wave Wireless Links Resilient Against Distributed Eavesdropper Attacks. *Nature Electronics*, In Press (2021).
- [21] S. Venkatesh, X. Lu, K. Sengupta, and B. Tang. 2020. Spatio-Temporal Modulated Millimeter-wave Antenna Arrays for Secure Wireless Links. In *2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting*. 1565–1566.
- [22] Xue Wu, Huaixi Lu, and Kaushik Sengupta. 2019. Programmable terahertz chip-scale sensing interface with direct digital reconfiguration at sub-wavelength scales. *Nature communications* 10, 1 (2019), 1–13.
- [23] A.D. Wyner. 1975. The wire-tap channel. *Bell system technical journal* 54, 8 (1975), 1355–1387.
- [24] N. Yang, L. Wang, G. Geraci, M. Elkhassan, J. Yuan, and M. Di Renzo. 2015. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Comm. Mag.* 53, 4 (2015), 20–27.