Energy- and Cost-Efficient Physical Layer Security in the Era of IoT: The Role of Interference

Zhongxiang Wei, Christos Masouros, Fan Liu, Symeon Chatzinotas, and Björn Ottersten

Abstract

IoT is emerging as the future evolution of the Internet, aiming to provide connectivity for everyone and everything. Since IoT is expected to carry important and private information, a high level of PHY security is critical for wireless communications in IoT, as a complement for traditional security techniques that are employed at high layers. In this overview, we examine the recent interest in energy-efficient and cost-efficient PHY solutions for securing downlink IoT transmission through interference exploitation. This exciting line of research departs from conventional interference cancellation, and judiciously employs the inherent interference as a useful element for LUs while obstructing the eavesdropping of information. We first discuss the concept of CI, and then elaborate the fundamental CI signal design that employs the traditionally undesired interference as a constructive element to LUs while ensuring they are destructive to potential Eves. Subsequently, we illustrate several low-hardware-cost techniques to inherit the advantage of CI in an energy- and cost-efficient manner, from the perspective of HBF and DM. This family of techniques brings a disruptive vision of interference management for securing wireless communications with an eye on low-cost and hardware-constrained devices tailored for IoT systems.

Introduction

The Internet of Things (IoT) builds the potential for the emerging Industry 4.0 and smart cities. With uniquely identifiable devices capable of wirelessly communicating, billions of devices are able to sense and interact with everything and everyone. The vision of IoT is to serve as a fundamental platform for transmission of important and private information, such as e-health data, infrastructure monitoring, and control messages of Industry 4.0. However, the broadcast nature of wireless communications inflicts an unprecedented vulnerability to cyber-crime, and high levels of security and privacy have become indispensable in IoT [1].

Traditionally, cryptographic techniques and associated protocols are normally employed at the upper layer of networks, assuming the physical layer (PHY) has already been established and provides an error-free link. Nevertheless, in large-scale IoT systems, the secret key distribution and management may be expensive and vulnerable to malicious attacks [2]. Hence, the ciphering and authentication protocols may be restrictive in IoT devices featuring small size and low cost. Furthermore, the premise of cryptographic schemes relies on the condition that the eavesdroppers (Eves) have limited processing capability, which is constantly being surmounted due to the growth of computational power and quantum computing. Most importantly, while the data itself is encrypted, Eves can still receive and analyze the traffic patterns to decipher useful information [3]. Thus, security threats start from the acquisition of data, which necessitates complementary security solutions that reside at a lower layer.

Recently, PHY security, an information-theory-based methodology, has been studied as a complementary measure to upper-layer techniques [3]. It has been shown that:

- The intrinsic PHY randomness of wireless channels, such as channel fading and interference, can be exploited to transmit data confidentially to legitimate users (LUs) while degrading the receiving quality of potential Eves.
- By preventing the signal detectability at Eves directly, it does not rely on limitations of Eves' computational resources; conventional cryptography is imminently vulnerable due to the rapid development of quantum computing.
- It does not rely on the higher-layer cryptographic/decryption, and thus releases the difficulties in the secrecy keys distribution and management in large-scale IoT systems.
- The achieved security performance can be quantified precisely with appropriately designed precoding and coding approaches.

Encompassing a number of key designs, PHY security has the potential to be one of the most effective forms of securing IoT communications.

The research on PHY security ranges from information-theoretic studies to protocol designs. Table I provides a brief summary of the most popular PHY security techniques. Of these techniques, some require a relatively large number of antennas for beamforming [4], bit-flipping, and noise aggregation [5]. Some utilize cooperative jamming and graph theory [2] with the help of external nodes. Some rely on additional proto-

The authors examine the recent interest in energy-efficient and cost-efficient PHY solutions for securing downlink IoT transmission through interference exploitation. This exciting line of research departs from conventional interference cancellation, and judiciously employs the inherent interference as a useful element for LUs while obstructing the eavesdropping of information.

Zhongxiang Wei, Christos Masouros, and Fan Liu are with University College London; Symeon Chatzinotas and Björn Ottersten are with the University of Luxembourg.

Digital Object Identifier: 10.1109/MCOM.001.1900716

PHY Security Techniques	Design Principles	Pros	Cons	Cost- and Power-Efficiency	Interference Management
Covert communication [7]	Hiding communication in interference	Providing covertness and stealth	Additional power on generating noise and interference	Low power-efficiency	(i) The transmitted signal is treated as infinite Gaussian signal. (ii) The correlation among the signal and channels is *NOT* exploited. (iii) Inference is always considered as a harmful element. (iv) and its effect needs to be mitigated as much as possible by providing time-, code-, frequency-, or spatiality-orthogonality. (v) More resources, i.e., subchannels, time slots, or antennas, are needed for providing strict orthogonality.
Cooperative jamming [2]	Generating jamming signal from relay or external nodes	Easing transmission power at source	Additional power consumption at assistant node	Low cost-efficiency	
Anti-attack [1]	Frequency hopping, Jammer detection, etc.,	Applicable for active Eves	Requirement of cooperation with LUs	Moderate cost- and power-efficiency	
Graph theory [2]	Secrecy graph formulation and optimization	No requirement on number of transmit antennas	Incompatibility with small scale networks	Low cost-efficiency	
Beamforming [4]	Maximising gain towards LUs	High data rate at LUs	High leakage towards Eves	Moderate cost- and power-efficiency	
	Zero-forcing towards Eves	Strict PHY security at Eves	Degraded receiving performance at LUs		
	Maximizing secrecy rate	Striking trade-off between LUs' performance and security against Eves	High computational complexity		
AN [3]	Isotropic manner	No requirement of Eves' CSI	Additional power consumption on AN	Low power-efficiency	
	Spatial manner	Energy-efficient than isotropic manner	Requirement of Eves' CSI		
Compressed sensing [5]	Multiplying sparse signal with measurement matrix	No expenditure on additional power	Measurement matrix available at LUs but unavailable to Eves, and non-negligible overheads incurred	Moderate cost- and power-efficiency	
Bit flipping [5]	Sending the bit-flipped data, i.e., false data, to interfere Eves	Low implementation complexity	Waste of transmission power and bandwidth on sending false data	Low power-efficiency	
PHY encryption [6]	Secret key generation at PHY	Simpler than the construction of codes for the wiretap channel	Agreement among the communication parties on the generated keys	Moderate cost- and power-efficiency	
Constellation rotation [5]	One dimension of the complex-valued signal for carrying information, and the other dimension for sending AN	Constellation based scheme	Reduced constellation size	Low power-efficiency	
Noise aggregation [5]	Use successfully transmitted symbol as key to encrypt the subsequent symbols	No additional power on AN	Requiring LU's channel advantageous over Eves' channel	Moderate cost- and power-efficiency	

Table 1. Brief summary of research on PHY security.

cols between transmitter and LUs for compressed sensing [5] and PHY encryption [6]. Some transmit the confidential signal under intentionally generated artificial noise (AN) [3] and covert communication [7]. Some address PHY security at the cost of reduced constellation size [5]. These techniques have specific advantages or disadvantages, whereas their application in IoT is still restrictive. This is because:

- A large number of devices in IoT feature small size, low cost, and low power consumption, as illustrated in Fig. 1. Nevertheless, the majority of the aforementioned techniques either incur additional power for generating AN, require a large number of antennas, or need external help nodes. All these factors can be hardware-demanding and energy-consuming in IoT devices.
- For typical scenarios in IoT, design metrics are focused on low power and high energy efficiency (EE), as opposed to throughput maximization. Hence, the traditional secrecy rate-maximization-oriented designs may be incongruous. Accordingly, power- and hardware-efficient designs have been the focus of recent research for IoT.

- The inherent interference in a multi-user environment, a critical resource, is not fully exploited in the design of PHY security techniques. Considering the massive connection capability of IoT, multi-user interference becomes a fundamental limiting factor for satisfying quality of service (QoS) of LUs, and hence strictly suppressing interference inevitably requires more resources, such as more antennas or sub-channels for providing strict orthogonality. A new family of techniques based on the constructive/destructive interference classification shown in Fig. 1 have been developed to treat the rich interference as a useful element and appropriately balance the LUs' QoS and PHY security against Eves.

Motivated by the aforementioned issues, the purpose of this article is to overview the energy- and cost-efficient techniques in accordance with the characteristics of IoT. Starting from examining the notation of constructive interference (CI) below, the validity and extensions of CI-based PHY security into hardware-constrained scenarios are then investigated, that is, hybrid beamforming (HBF) and direction modulation (DM). Open challenges are envisaged, and a conclusion is given in the final section.

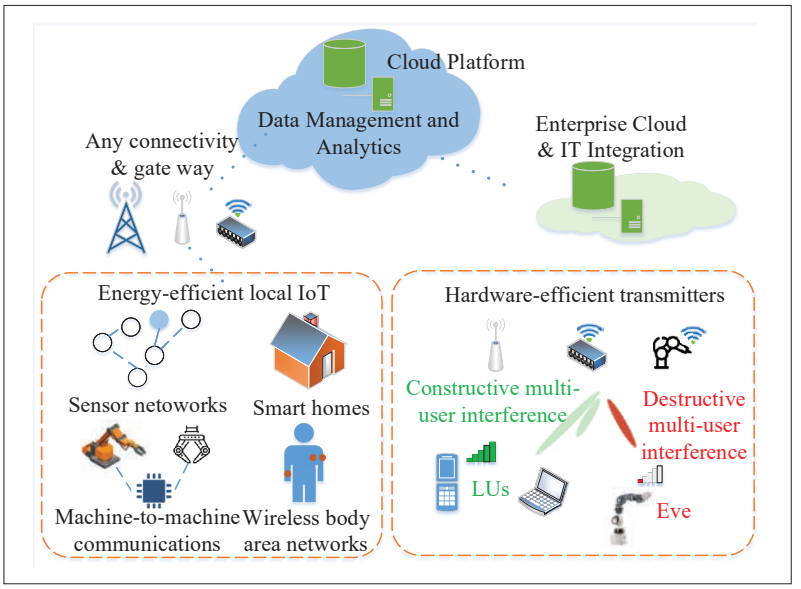

Figure 1. In IoT systems, low-power, low-hardware-cost, and low-complexity PHY security techniques are preferable through the upcoming paradigm of interference exploitation. A new family of techniques based on the constructive/destructive interference classification have been developed that treat the rich interference as a green signal source to LUs while keeping it destructive to Eves.

CI-Based PHY Security

Let us start by demonstrating the concept of CI, and we can then elaborate the fundamental CI signal design for addressing PHY security.

The Concept of CI

Conventionally, interference is considered as the most harmful factor limiting LUs' receiving performance. By leveraging the channel reciprocity and exploiting the characteristics of IoT communications, such as joint active devices detection and channel estimation, and sparsity pattern of data transmission, channel state information (CSI) acquisition can be efficient in IoT [8]. Hence, with CSI available at the transmitter, multi-user interference can be predicted and characterized prior to transmission. This is then used for mitigating interference at the LU side. That is, the aim of conventional interference cancellation techniques is to contain the received symbols within a region around the nominal point in the modulated signal constellation [9]. This idea is indeed optimal from a statistical viewpoint. Since the transmitted signal is treated as an infinite Gaussian signal, any interference adds perturbation to the signal and harms performance.

Nevertheless, since the transmitted symbols are also available at the transmitter, it is judicious to jointly utilize the spatial cross-coupling between the users' channel and the transmitted symbols [10]. Aided by symbol-level precoding [9], we can rotate, rather than mitigate, the correlation between the transmitted data so that the interfering signal is aligned with the signal of interest at each receiver [10]. That is, CI precoding depends on both the users' channels and transmitted symbols, which is completely different from conventional designs, including zero-forcing (ZF), minimum mean squared error (MMSE), power minimization, and signal-to-interference-plus-noise ratio (SINR) balancing precoders, which are only related to channels but independent of the desired symbols. Hence, there is scope to make interference constructive to the LU while still destructive to Eves for addressing PHY security, which is essentially beneficial to systems in terms of EE [11].

CI Signal Design

The fundamental principle of CI is to utilize interference as a constructive element rather than cancelling it, and CI can push LUs' signals away from the detection thresholds of the signal constellation. As a result, the increased distance to the detection threshold can improve LUs' SINR [11]. In other words, lower transmission power is consumed to achieve a target performance at LUs, and hence higher EE is endorsed.

To clarify the above fundamental concept, we illustrate a generic CI-based precoding guideline in Fig. 2. First, with the input signal and the adopted constellation scheme, interference characterization can be performed at the transmitter side. The constructive regions of each constellation are denoted by the green shaded areas. To be specific, given the decision bounds in each modulation constellation, interference is constructive when it pushes the received signals away from the bounds and destructive when it pushes the received signal toward or across the decision bounds. For binary phase shift keying (BPSK), since the decision threshold is the imaginary axis, the interference is constructive when it has the same sign as the target signal. The decision thresholds for quadrature phase shift keying (QPSK) modulation are the real and imaginary axes, and thus CI should push the desired signal away from both the real and imaginary axes. In a similar fashion, interference can be characterized for any constellation scheme. Detailed studies and explicit mathematical criteria can be found in [10]. Based on the CI characterization, judicious precoding can be employed to make interference constructive for LUs, and

HBF involves a low dimensional baseband precoding, followed by high dimensional analogue precoding. A recent line of research extends CI to HBF architectures to further reduce the hardware cost and also the circuit power consumption [14]. Nevertheless, HBF's ability on addressing PHY security is less exploited.

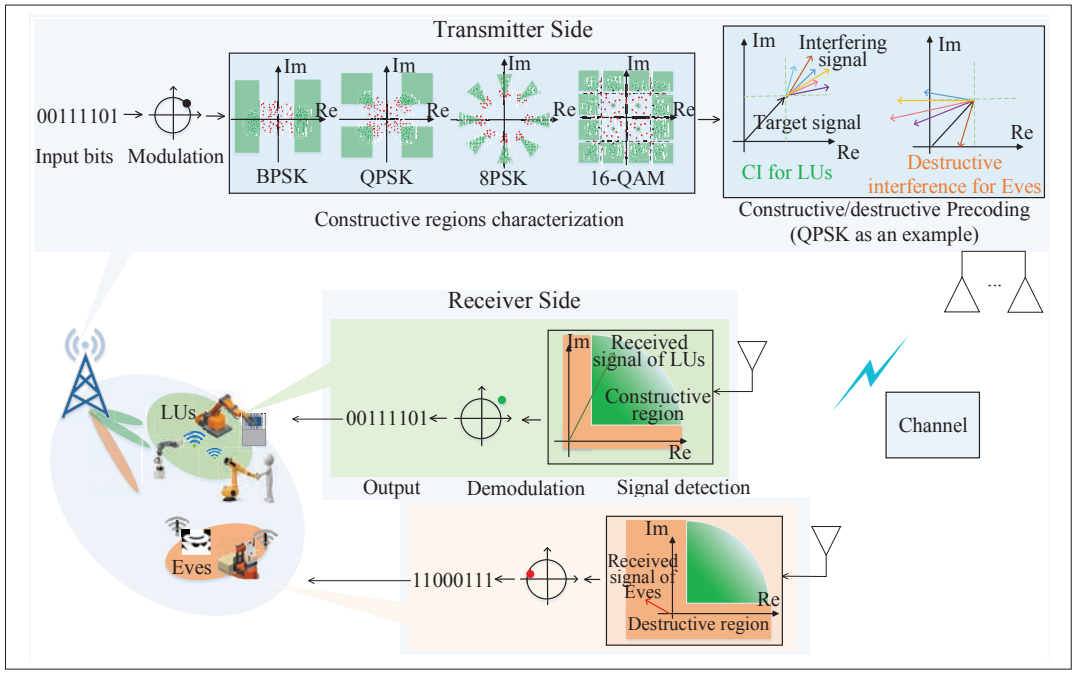

Figure 2. A generic CI-based precoding guideline for IoT. The CI pushes the resultant symbol away from the original decision threshold of the constellation, and hence the received signal of LUs falls into constructive regions (green area). On the other hand, interference can be kept destructive to potential Eves, and the received signal of Eves is pushed into destructive regions (orange area). At the transmitter side, modulation is first performed with the input bits, and then constructive regions are characterized for the adopted modulation scheme. Finally, symbols are precoded based on the concept of CI and propagated to receivers [12]. At the receiver side, conventional signal detection and demodulation are simply performed to obtain the output bits. Evidently, the design thread at the transmitter and receiver is exactly the same as the hardware realization of CI precoding in the NB-IoT platform [12].

hence the received signal of LUs is pushed into constructive regions (the green regions). By exploiting CI, the rich interference becomes a green signal source for improving LUs' receiving performance. In other words, to achieve a target performance at LUs, lower transmission power is needed as interference contributes constructively rather than being mitigated. This has been shown to yield an up to 6.5 dB gain in the transmit power over the traditional ZF, maximum ratio transmission, and power minimization precoding schemes in small-scale systems [9].

On the other hand, to address PHY security, the interference is designed to be destructive to Eves, whose signal is intentionally pushed into destructive regions (the orange regions). Since the signal in the destructive regions points to a different constellation point from the confidential signal, the Eves' receive performance is intentionally degraded. In the scenario when the Eve's CSI is unknown by the transmitter, one can only tailor CI for the LUs. Since CI is only dedicatedly designed for the LUs, the received signal of a potential Eve is randomized across the constellation panel due to channel disparity, also leading to a high symbol error rate [13]. That is, the beam leakage acts as the null-space noise to jam and distort the constellation of the same signals in all directions other than the desired ones relying on the spatial diversity of the channel simultaneously. In summary, PHY security can be explicitly guaranteed with Eves' CSI, while being addressed in a statistical manner without Eves' CSI. Furthermore, it does not incur additional power on generating AN.

CI-Based Hardware-Efficient PHY Security

In this section, we extend the concept of CI into hardware-efficient designs from the perspectives of HBF and DM. Due to page limit, we illustrate the CI-based HBF design with Eves' CSI and then CI-based DM design without Eves' CSI.

Hybrid Beamforming

The implementation of fully digital beamforming (DBF) is prohibitive from both the cost and power consumption perspectives, since it requires dedicated radio frequency (RF) chains per antenna element. On the feasibility of CI exploitation with high hardware efficiency, one approach is to reduce the RF chains through analog architectures that involve phase shifters (PSs). Accordingly, HBF involves a low-dimensional baseband precoding, followed by high-dimensional analog precoding. A recent line of research extends CI to HBF architectures to further reduce the hardware cost and also the circuit power consumption [14]. Nevertheless, HBF's ability on addressing PHY security is less exploited.

CI-Based PHY Security in HBF: Optimal design of HBF may be nontrivial, and generally the resulting optimization problems are non-convex. A common approach for HBF design is to decompose the designs of analog and digital beamformer. For example, one can first optimize the analog beamformer, and then, for the fixed analog beamformer, the optimal digital beamformers can be properly designed. In a more optimal manner,

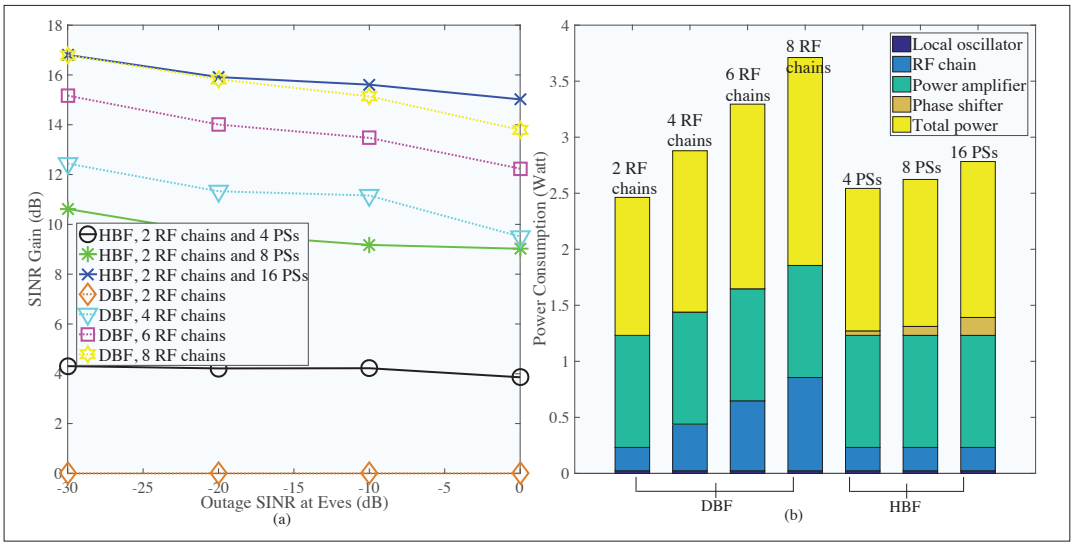

Figure 3. LU's SINR gain performance over the benchmark (DBF, equipped two RF chians): a) with a pre-set outage SINR imposed against the Eves for addressing PHY security, LUs' SINR gain achieved by HBF approaches that of DBF; b) power consumption of the HBF structure is significantly reduced over DBF counterpart, due to the less numbers of RF chains.

the analog beamformer and digital beamformer are iteratively optimized assuming the other part being fixed.

Here, we illustrate a simple HBF design to inherit the legacy of CI in a hardware- and power-efficient manner. The Eves' CSI is assumed to be known at the transmitter, and hence we can constrain a low SINR of Eves from −30 dB to 0 dB for PHY security purpose, by intentionally imposing destructive interference for the Eves. We employ a hardware-efficient codebook-based analog beamforming design. To be specific, analog beamforming is first selected to maximize the inner product with their associated channel vector. Afterward, it is easy to merge the effect of the analog beamformer into the channels and obtain equivalent channels for LUs and Eves. Hence, the subsequent DBF design is to exploit the spatial correlation among the transmitted data and users' channels for employing CI-based precoding, as clarified previously. In Figs. 3a and 3b, the LUs' SINR gain and power consumption of different configurations are demonstrated, benchmarked by the DBF equipped with two RF chains. As observed, with a pre-set outage SINR constraint at Eves, HBF equipped with 2 RF chains and 16 PSs even outperforms DBF equipped with 8 RF chains in terms of LUs' achieved SINR. With a moderate number of PSs, the gain of HBF equipped with 2 RF chains and 8 PSs is only 1 dB lower than DBF equipped with 4 RFs. More importantly, since the power incurred by PSs in HBF contributes trivially to the power consumption compared to RF chains, the power consumption of HBF is significantly reduced over DBF. This advantage is more pronounced comparing HBF equipped with 2 RF chains and 4 PSs and DBF equipped with 2 RFs in Fig. 3b, where the HBF almost consumes the same power but achieves 4 dB SINR gain over the DBF counterpart.

Directional Modulation

By the aforementioned techniques, the required number of RF chains should be no smaller than the total number of data stream for multi-user access. To this end, a more hardware-efficient CI implementation technique, namely DM, is promising in securing IoT systems, where expensive and power-consuming RF chains are not required [13]. With the DM technique, symbols' modulation happens at the antenna level instead of at the baseband by conventional beamforming design, and the received beam pattern at LUs' receivers is treated as a spatial complex constellation point [13]. Hence, DM constructs the received symbols at the users directly, while relying on the spatial diversity of the channel to simultaneously distort the constellation of the same signals in all directions rather than the desired ones. Generally, there are two main designs for realizing DM, one based on actively driven elements (e.g., PSs and power amplifier) and the other based on parasitic antennas [13]. Regardless of structures, the hardware cost of a DM transmitter can be significantly reduced compared to conventional DBF or HBF structure, as illustrated in Fig. 4.

CI-Based DM Design: The initially strict phase design requires the constructed signal to have exactly the same phase and amplitude of the desired symbol. As a result, the degrees of freedom (DoFs) at the transmitter are limited, and consequently LUs' receiving performance is degraded [13]. To improve the receiving performance, the concept of CI can be brought into DM to relax the strict phase requirement. In particular, the constructed signal does not necessarily align with the intended symbols, but is pushed away from the detection thresholds of the signal constellation. In this case, a higher level of DoFs at the transmitter is endorsed, and less transmission power is required compared to the strict phase DM design.

On the other hand, when addressing PHY security against potential Eves, channel disparity among the LUs and Eves can be utilized to randomize the Eves' received symbols. That is, since confidential symbols are only dedicatedly tailored for LUs, the beam leakage distorts the constellation in other directions, relying on the spatial diversity of the channels. An example is

There are two main designs for realizing DM, one based on actively driven elements (e.g., PSs and power amplifier) and the other based on parasitic antennas [13]. Regardless of structures, the hardware cost of a DM transmitter can be significantly reduced compared to conventional DBF or HBF structure.

The increased number of devices complicates the networking, and necessities heterogeneous types of structures and transmissions. With the increased number of devices, the security and privacy requirements are intended to be more personalized. For example, public broadcast may have low privacy requirement, whereas some personal information have high requirement on confidentiality.

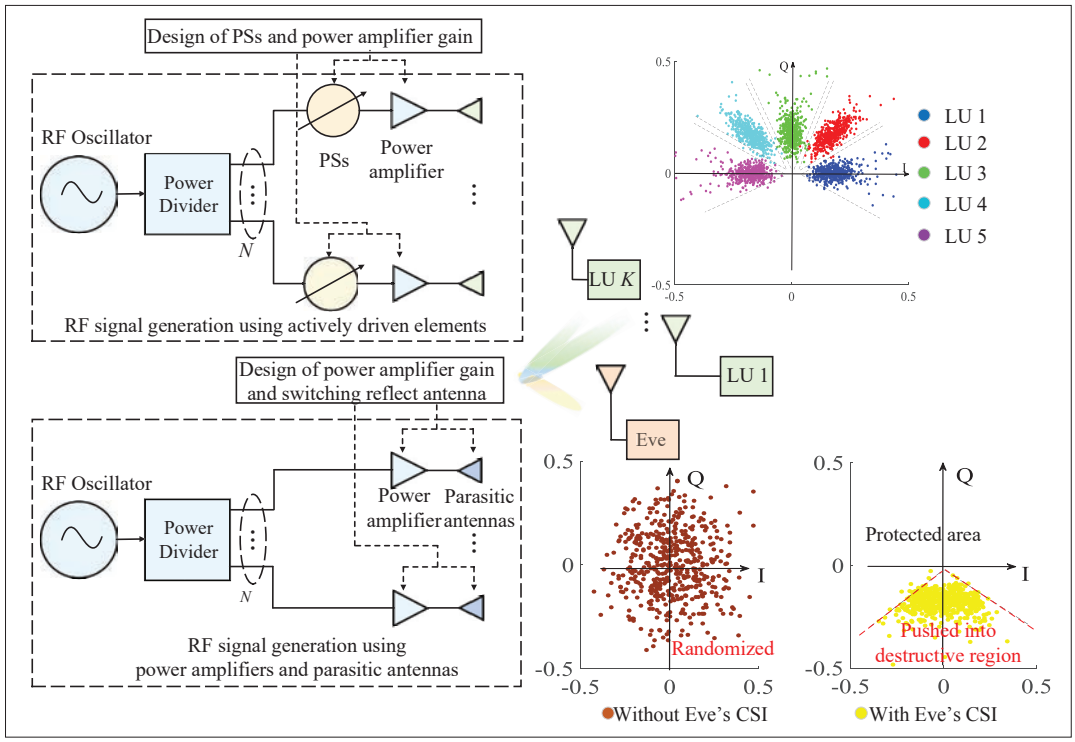

Figure 4. RF signal can be directly modulated at the antenna level by use of driven elements or parasitic antennas. Assume there are five LUs, and their desired symbols are pushed into CI regions. On the other hand, when addressing PHY security, the Eves' received signal (denoted by brown dots) is scrambled across the constellation panel due to the channel disparity. With Eves' CSI, a more dedicated design can be achieved by intentionally locating the Eves' received signal (denoted by yellow dots) into destructive regions.

illustrated by Fig. 4, where an actively driven elements-based DM structure is utilized. Assume there are five LUs and their desired symbols are generated by 8-PSK. By adaptively adjusting the power and phases at the transmitter side, the constructed symbols of LUs are indeed located in the constructive region, denoted by colored dots. As a comparison, due to the channel disparity, the received signals at the Eves (denoted by brown dots) are completely scrambled. Nevertheless, as aforementioned, PHY security may not be explicitly addressed in this case, especially when potential Eves' channels are strongly correlated with that of LUs. On the contrary, when the Eves' CSI is known, we can dedicatedly construct the Eves' received signal into destructive regions, that is, those regions in the constellation that are not occupied by the LUs. Since the constructed artificial symbols at Eves (denoted by yellow dots) are intentionally designed to be different from the confidential symbols of the target LUs, the Eves' symbol error rate is further deteriorated, and PHY security performance can be guaranteed.

Open Challenges and Future Works

The topic of energy- and cost-efficient PHY security is still broadly open for research and could be extended in many interesting directions:

Delay and Reliability-Aware PHY Security: Some emerging applications of IoT, such as co-robot operation in Industry 4.0 and mixed reality in remote medical interaction, require low end-to-end latency on the order of milliseconds and high system reliability (packet error rate) on the order of 10^{-6} to 10^{-9}. These applications arise from ultra-reliable low-latency communications (URLLC), where dedicated protocols are preferable to satisfy the stringent requirements. For example, short packet structure and incompatibility of hybrid automatic repeat request retransmissions make PHY security design more distinct from conventional systems. Evidently, joint optimization of multiple objectives of security, reliability, and latency is not trivial at a network level. A possible solution is cross-layer optimization ranging from PHY to network layer, that is, frequency/time/precoding design at the PHY layer, packet scheduling at the medium access control (MAC) layer, and routing design at the network layer. Nevertheless, such complicated designs incur high complexity, high power, and complicated protocol. Besides, the impact of exploiting CI on the above performance-vs-latency trade-offs and with small packets has yet to be explored.

Heterogeneous Networking and Personalized Security: The increased number of devices complicates networking, and necessities heterogeneous types of structures and transmissions. With the increased number of devices, the security and privacy requirements are intended to be more personalized. For example, public broadcast may have a low privacy requirement, whereas some personal information has a high requirement for confidentiality. A possible solution is to arrange various levels of security and apply appropriate PHY security techniques for different services. This again requires fundamental analysis and new metrics for designing and evaluating the overall system PHY security performance, especially under the provision of CI-based heterogeneous networks.

PHY Security from the Perspective of Intelligent Eves: Recently, the concept of machine learning (ML) has been leveraged at the transmitter side to enhance PHY security against Eves, and related research has been conducted for large-scale cellular networks, IoT, and industrial wireless cyber-physical systems, from the perspectives of secure precoding, relay selection, authentication, and wiretap code designs [15]. Nevertheless, it has been assumed that the potential Eves are equipped with simple detectors, and the detection rule is simply to choose the nearest constellation point for demodulation. On the contrary, Eves equipped with abundant computing ability are also able to analyze the received signal in a smarter way aided by ML, defined as intelligent-Eves. An intelligent-Eve could exploit the statistical characteristics of the received signal and then employ an ML-based detector to analyze the received signal, thereby refining its symbol error rate performance. Hence, it is demanding to rethink the CI-based techniques from the perspective of intelligent-Eves, and more robust security techniques need to be developed, especially in the colluding intelligent-Eves scenario.

Conclusions

This article has overviewed a distributive approach taking advantage of interference in hardware-, size-, and power-constrained IoT devices and applications. We have discussed the potential of making use of interference as a green source to LUs while keeping it destructive to potential Eves. Furthermore, the validation of CI-based PHY security has been examined in low-hardware-cost systems. The reviewed novel solutions can provide energy-efficient and hardware-efficient secure transmission for the downlink of IoT, offering a broad field for utilizing interference to secure the upcoming IoT. A number of challenges related to emerging applications are still present, and essential work is needed to bridge the gap between theory and implementations, which holds the promise of exciting research in the years to come.

Acknowledgment

This work was supported by the Engineering and Physical Sciences Research Council, U.K., under Project EP/R007934/1.

References

[1] Y. Qu *et al.*, "Privacy of Things: Emerging Challenges and Opportunities in Wireless Internet of Things," *IEEE Wireless Commun.*, vol. 25, no. 6, Dec. 2018, pp. 91–97.
[2] A. Mukherjee *et al.*, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, Feb. 2014, pp. 1550–73.
[3] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, June 2008, pp. 2180–89.
[4] X. Chen, D. Ng, and H. Chen, "A Survey on Multiple-Antenna Techniques for Physical Layer Security Security, *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 2, Nov. 2016, pp. 1027–53.
[5] L. Sun and Q. Du, "A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions," *Entropy*, vol. 20, no. 10, July 2018, pp. 1–15.
[6] J. Zhang *et al.*, "Efficient Key Generation by Exploiting Randomness From Channel Responses of Individual OFDM Subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, June 2016, pp. 2578–88.
[7] Z. Liu *et al.*, "Covert Wireless Communications in IoT Systems: Hiding Information in Interference," *IEEE Wireless Commun.*, vol. 25, no. 6, Dec. 2018, pp. 46–52.
[8] T. Jiang et al., "Joint Activity Detection and Channel Estimation for IoT Networks: Phase Transition and Computation Estimation Trade Off," *IEEE Internet of Things J.*, vol. 6, no. 4, Aug. 2019, pp. 6212–25.
[9] M. Alodeh *et al.*,"Constructive Multiuser Interference in Symbol Level Precoding for the MISO Downlink Channel," *IEEE Trans. Signal Processing*, vol. 63, no. 9, May 2015, pp. 2239–52.
[10] C. Masouros and G. Zheng, "Exploiting Known Interference as Green Signal Power for Downlink Beamforming Optimization," *IEEE Trans. Signal Processing*, vol. 63, no. 14, July 2015, pp. 3628–40.
[11] M. Khandaker *et al.*, "Constructive Interference Based Secure Precoding: A New Dimension in Physical Layer Security," *IEEE Trans. Info. Foren. Sec.*, vol. 13, no. 9, Sept. 2018, pp. 2256–68.
[12] T. Xu *et al.*, "Constructive Interference Precoding for Reliable Nonorthogonal IoT Signalling," *Proc. IEEE INFOCOM*, Paris, France, 2019.
[13] A. Kalantari *et al.*, "Directional Modulation via Symbol-Level Precoding: A Way to Enhance Security," *IEEE J. Sel. Topics Signal Processing*, vol. 10, no. 8, Dec. 2016, pp. 1478–93.
[14] G. Hegde, C. Masouros, and M. Pesavento, "Interference Exploitation-Based Hybrid Precoding With Robustness Against Phase Errors," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, July 2019, pp. 3683–96.
[15] F. Restuccia, S. D. Oro, and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," *IEEE Internet of Things J.*, vol. 50, no. 6, Dec. 2018, pp. 4829–42.

Biographies

Zhongxiang Wei is a research associate in electrical and electronics engineering at University College London. He received his Ph.D. degree in electrical and electronics engineering from the University of Liverpool, United Kingdom, in 2017. From March 2016 to March 2017, he was with the Institution for Infocomm Research, Agency for Science, Technology, and Research (A*STAR), Singapore, as a research assistant. His research interests include constructive interference design, green communications, full-duplex, millimeter-wave communications, and algorithm design.

Christos Masouros is a full professor in the Department of Electrical and Electronic Engineering, University College London. He received his Ph.D. in electrical and electronic engineering from the University of Manchester, United Kingdom, in 2009. He held a Royal Academy of Engineering Research Fellowship between 2011 and 2016. His research interests lie in the field of wireless communications and signal processing with particular focus on green communications, large-scale antenna systems, and interference exploitation. He was the recipient of Best Paper Awards at IEEE GLOBECOM 2015 and IEEE WCNC 2019. He is an Editor for *IEEE TCOM* and *IEEE TWC*. He has been an Associate Editor for *IEEE COML* and a Guest Editor for *IEEE JSTSP*.

Fan Liu received his Ph.D. and B.Eng. degrees from Beijing Institute of Technology, China, in 2018 and 2013, respectively. He was a visiting Ph.D. student in the Department of Electronics and Electrical Engineering, University College London between 2016 and 2018, where he is currently a Marie Curie Research Fellow. He was the recipient of the 2019 Best Ph.D. Thesis Award of the Chinese Institute of Electronics. His research interests include precoding designs for MIMO systems, signal detection and estimation, and convex optimization.

Symeon Chatzinotas is currently a full professor and deputy head of the SIGCOM Research Group at SnT University of Luxembourg. He received his M.Eng. degree in telecommunications from the Aristotle University of Thessaloniki, Greece, in 2003, and his M.Sc. and Ph.D. degrees in electronic engineering from the University of Surrey, United Kingdom, in 2006 and 2009, respectively. He was a co-recipient of the 2014 IEEE Distinguished Contributions to Satellite Communications Award, the CROWNCOM 2015 Best Paper Award, and the 2018 EURASIC JWCN Best Paper Award. He has authored more than 350 technical papers in refereed international journals, conferences, and scientific books.

Björn Ottersten received his Ph.D. degree in electrical engineering from Stanford University, California. He is director of the Interdisciplinary Centre for Security, Reliability and Trust at the University of Luxembourg. He has received the IEEE Signal Processing Society Technical Achievement Award, the IEEE Communications Society Satellite Communications Distinguished Service Award, the EURASIP Group Technical Achievement Award, and is a two-time recipient of the European Research Council advanced research grant. His research interests include signal processing, wireless communications, radar systems, and computer vision.

The reviewed novel solutions can provide energy-efficient and hardware-efficient secure transmission for the downlink of IoT, offering a broad field for utilizing interference to secure the upcoming IoT. A number of challenges related to emerging applications are still present, and essential work is needed to bridge the gap between theory and implementations.