PROCEEDINGS A

royalsocietypublishing.org/journal/rspa

Research

Cite this article: Khadr MH, Elgala H, Rahaim M, Khreishah A, Ayyash M, Little T. 2021 Machine learning-based security-aware spatial modulation for heterogeneous radio-optical networks. *Proc. R. Soc. A* **477**: 20200889.
https://doi.org/10.1098/rspa.2020.0889

Received: 13 November 2020
Accepted: 9 March 2021

Subject Areas:
artificial intelligence, electrical engineering

Keywords:
physical layer security, machine learning, heterogeneous networks, optical wireless communications, wireless communications

Author for correspondence:
Monette H. Khadr
e-mail: mkhadr@albany.edu

Machine learning-based security-aware spatial modulation for heterogeneous radio-optical networks

Monette H. Khadr[1], Hany Elgala[1], Michael Rahaim[2], Abdallah Khreishah[3], Moussa Ayyash[4] and Thomas Little[5]

[1]Electrical and Computer Engineering Department, University at Albany, Albany, NY, USA
[2]Engineering Department, University of Massachusetts Boston, Boston, MA, USA
[3]Electrical and Computer Engineering Department, New Jersey Institute of Technology, Newark, NJ, USA
[4]Department of Chemistry, Physics and Engineering Studies, Chicago State University, Chicago, IL, USA
[5]Department of Electrical and Computer Engineering, Boston University, Boston, MA, USA

MHK, 0000-0001-6913-2253; MA, 0000-0003-0868-143X

In this article, we propose a physical layer security (PLS) technique, namely security-aware spatial modulation (SA-SM), in a multiple-input multiple-output-based heterogeneous network, wherein both optical wireless communications and radio-frequency (RF) technologies coexist. In SA-SM, the time-domain signal is altered prior to transmission using a key at the physical layer for combating eavesdropping. Unlike conventional PLS techniques, SA-SM does not rely on channel characteristics for securing the information, as its perception is self-imposed, which allows its adoption in radio-optical networks. Additionally, a novel periodical key selection algorithm is proposed. Instead of having multiple keys stored in the nodes, by using off-the-shelf and low-complexity machine learning (ML) methods, including a support vector machine, logistic regression and a single-layer neural network, SA-SM nodes can estimate the used key. Results show

THE ROYAL SOCIETY PUBLISHING

that a positive secrecy capacity can be achieved for both the RF and optical links by using 1000 different keys, with a minimal signal-to-noise ratio penalty of less than 5 dB for the legitimate user using SA-SM versus conventional transmission at a bit-error-rate of 10^{-4}. The analysis also includes computational time and classification accuracy evaluation of the various proposed ML techniques using different hardware architectures.

1. Introduction

Radical next-generation networking concepts are gaining attention in academic and commercial communities to satisfy the unprecedented data rate demands for cutting-edge applications [1]. Next-generation networks are expected to intelligently satisfy users' demands while satisfying the confidentiality requirement of the user. Confidentiality can be defined as the ability to restrict data interpretation to legitimate users only, while averting unauthorized entities from accessing the information [2]. Owing to the broadcast nature of wireless transmission, the wireless interface is within reach of both legitimate and malicious users. Eavesdropping attacks are the most popular type of threat that affect network confidentiality [3]. To combat eavesdropping, security approaches can be applied at every layer of the network stack, including encryption and authentication protocols in the upper layers as well physical-layer (PHY) mechanisms [4]. Physical-layer security (PLS) is an emerging technology that encompasses approaches proposed for securing wireless communications at the PHY. In PLS, the core idea is to use the attributes of wireless channels, such as noise or fading, to model effectively secure transmission schemes.

The introduction of new applications, such as Internet-of-Things (IoT), with their computational complexity and power limitations, has called attention to the importance of PLS, as the traditional cryptographic methods are normally computationally complex. With the development of cutting-edge hardware architectures, such as tensor processing units (TPUs) and graphical processing units (GPUs), machine intelligence has emerged from laboratory curiosity to practical implementation. In wireless communications, machine intelligence has been used in signal detection [5–7], channel estimation [8,9], channel encoding and decoding [10–12] and channel state information (CSI) sensing [13]. By applying machine learning (ML) technology, PLS approaches can be further optimized in comparison with non-ML-based conventional security technologies. Therefore, the application of ML for PHY design and optimization needs to be deeply investigated to design networks that are more agile, intelligent and robust.

Perfectly secure transmission in a discrete memoryless wiretap channel was first examined by Wyner, assuming a source and a destination in the presence of an eavesdropper [14]. Wyner's analysis was extended from a discrete memoryless wiretap channel into a Gaussian wiretap channel in [15]. The analysis in [15] introduced the metric secrecy capacity, which can be interpreted as the disparity between the channel capacity of the legitimate user and the eavesdropper. According to the secrecy capacity definition, a transmission is considered secure as long as the secrecy capacity does not fall below zero, and thus an eavesdropper would not be able to fully intercept the source's transmission. In order to enhance system confidentiality, sophisticated signal processing techniques are designed to elevate secrecy capacity. These techniques include security-oriented beamforming [16,17], artificial-noise-aided security [18,19], PHY secret key generation-based methods [20,21] and security diversity methods [22,23]. Considering secret key generation techniques, the premise is that the source encrypts the original data with the aid of an encryption algorithm and a secret key, which is exchanged between the source and the legitimate receiver only. Using classic channel estimation methods, legitimate users exploit their estimated CSI for secret key generation and agreement process. The legitimate receiver then decrypts the data using the preshared key. Hence, under the assumption that the eavesdropper lacks information of the secret key, the data reserve its confidentiality.

Currently, radio-frequency (RF) technology is suffering from a lack of free spectrum, and thus meeting the insatiable demand for data rates is becoming extremely challenging. To conform with this increase in demand, solutions such as complementing conventional RF technologies with various technologies, including optical wireless communications (OWCs), are emerging [24]. OWC technology conveys data in free space via optical radiation, and its wavelengths can range from infrared to ultraviolet, which includes the visible light spectrum [25]. The advantages of OWC include a large unlicensed spectrum and no interference with other technologies (i.e. RF), and it gives rise to the all-green communication aspiration. Hybrid networks, also known as heterogeneous networks (HetNets), which combine RF transmission with optical, not only offer unprecedented data rates but also improve system reliability and coverage area. Hence, radio-optical HetNets are starting to gain significant attention in the research community.

Most PLS techniques exploit the propagation characteristics of the wireless channel. When wireless data are transmitted by a source, multiple replicas of the signal with different delays and attenuation factors may be received at the destination arriving from different propagation paths caused by signal reflection, diffraction and scattering. In a setting that adopts multiple technologies, such as in the case of heterogeneous radio-optical networks, PLS techniques cannot depend on the unpredictability of the multipath propagation to defend the transmission because the optical channel is not rich scattering, unlike the RF channel. Hence, the unpredictability criterion is absent in optical transmission. Another approach is PHY-key-based techniques that adopt the concept of encryption and authentication based on the presence of a secret key; however, the encryption happens at the PHY. For these techniques, an efficient key management and distribution scheme is fundamental for network confidentiality. As a general scheme, there exists a key management server responsible for generating and managing the keys. The keys are then distributed among the end-users; however, the protection of keys in transit must be paramountly considered [26]. Additionally, key distribution results in network over-head owing to the exchange of keys over the network. An alternative is key predistribution models, where keys are stored in nodes before deployment, which are popular in a multiple of applications, including wireless sensor networks, because of their low computational complexity and scalability [27].

Multiple-input multiple-output (MIMO) is a key technology in current and, most probably, future wireless networks including HetNets, as it enhances the spectral and energy efficiencies of the system [28]. Spatial modulation (SM) is an emerging MIMO transmission method that regards the transmitter index as an additional stream of information [29]. In SM, the information bits are split into a portion that is modulated by signals and another that is conveyed in the transmitter index. Only one transmitter is active during symbol transmission, thus the data rate can be increased by a factor of $\log_2(N_T)$, where N_T is the number of available transmitters. SM-based PLS can be addressed using various approaches, including precoding, jamming and subset selection. There are also methods that are considered combinations of the aforementioned PLS approaches, such as the work in [30], which is considered a precoding plus jamming technique. Precoding techniques, such as [31–33], rely on engineering the precoding matrix coefficients based on CSI of both the legitimate user and eavesdropper to cause the signal to be perceived only by the legitimate user and be hidden from the eavesdropper. The major drawback of precoding approaches is the stringent requirement of CSI. Practically, networks can be oblivious to the presence of an eavesdropper, which makes eavesdropper CSI knowledge unachievable. Friendly jamming methods create artificial noise in the nullspace of the legitimate user, causing the eavesdropper to undergo destructive effects [34]. Jamming approaches, i.e. artificial noise, can be based on co-operative jamming, where multiple users aid each other to mitigate eavesdropping attacks [35,36]. It can also be based on a MIMO setting, where the legitimate users are equipped with multiple transmitters/receivers [37]. The drawbacks of jamming methods are their power inefficiencies and spectral efficiency losses, as the spatial bits are compromised owing to the use of transmitting elements as jamming elements. Lastly, transmitter subset selection methods choose a specific subset of transmitting elements to maximize either the signal-to-noise-ratio (SNR) or the Euclidean distance at the legitimate user [38,39]. Similar to jamming approaches,

they require CSI of the legitimate users, and they also share the loss in spectral efficiency as the number of bits that can be conveyed in the spatial domain are reduced as a result of the subset selection task.

SM has been extensively investigated in radio [40] and optical [41] wireless networks separately; however, addressing the security of SM-based systems in radio-optical HetNet deployments has received limited attention in the research community. The shift to higher frequencies causes the transmitted signals to propagate differently from in RF. Instead of optimizing both technologies separately, a technique that can be applied to multiple technologies is crucial in HetNets, as it enables common protocols to be deployed. Thus, when considering PLS techniques for radio-optical HetNets, the technique used must consider the decreased angle divergence of signals transmitted optically in comparison with RF transmission, which is still an under-investigated area of research. Generally speaking, there is a minimal amount of research that is dedicated to RF/optical HetNet security. To the authors' knowledge, a key distribution mechanism for radio-optical HetNets does not exist in the literature. Secrecy outage analysis of RF/optical hybrid networks and the derivation of analytical expressions for the exact and asymptotic secrecy outage probability (SOP) is presented in [42,43]; SOP can be described as the probability that the secrecy capacity is equal to zero. A zero-forcing beamforming strategy and a minimum power allocation algorithm is presented in [44]. In [44], the RF secrecy rate outperformed the optical link. As the eavesdropper got closer to the legitimate user, their optical channels became more dependent and their null spaces became very close. In contrast, RF transmission has a probabilistic channel model and the correlation between RF channels is much less than the optical case. A handover mechanism is given in [45] in which OWC is used as the primary technology and RF is used only if the primary technology fails to satisfy a positive secrecy rate limit. For [45], the case in which both technologies are used concurrently is not investigated. In wireless link pairing (WiLP) [46], the real and imaginary parts of a quadrature amplitude modulator (QAM) are separated. Then, the real part is sent over the RF link, while the imaginary part is sent over the optical link. Since both the RF and optical links are needed for signal reconstruction, if any of the links get blocked all the transmitted information will be lost.

Given the immense potential of radio-optical HetNets and the importance of eavesdropping mitigation in any network, this paper is dedicated to investigating a PLS technique proposed for MIMO-based radio-optical HetNets. This paper is an extended version of our previous work on security-aware spatial modulation (SA-SM) [47]. Unlike the aforementioned methods, SA-SM operates in a different manner. SA-SM disturbs the time-domain signal prior to transmission (at the PHY) using a key, which reduces the eavesdropper's channel capacity without influencing the legitimate user's channel capacity, which in return increases secrecy capacity. In this sense, SA-SM does not rely on channel characteristics for securing the information, as its perception is self-imposed; hence, it can be applied to both RF and optical technologies concurrently, and the security gain in both cases will be the same (as it is not channel reliant). We extend our previous analysis by introducing a novel key selection algorithm and applying various ML algorithms, including support vector machines (SVMs), logistic regression (LR) and a neural network (NN), to allow periodical PHY rekeying issued by a centralized source to ML-equipped nodes. Unlike other rekeying methods proposed in the literature, SA-SM's perception does not require keys to be exchanged between the centralized source and the communicating nodes. This perception not only protects keys from being intercepted in transit, but also eliminates rekeying overhead. Instead, SA-SM nodes can intelligently identify which key is chosen by the source, out of a fixed key pool, and decrypt the information accordingly. The main contributions of this work are as follows.

— This work is the first to investigate applying ML for PLS in radio-optical HetNets. The analysis includes computational time and classification accuracy evaluation of the various proposed ML techniques.
— To the best of the authors' knowledge, a key selection algorithm for RF–optical security does not exist. Additionally, we have based our analysis on well-known ML multi-class

classification approaches that are readily available off-the-shelf as hardware components that can be employed in practice.
— The implementation is executed using different hardware architectures, including GPUs, central processing units (CPUs) and TPUs, to conform with various application scenarios.

The remainder of the paper is organized as follows. Section 2 details the radio-optical HetNet system model, while §3 describes the proposed SA-SM technique. The key selection algorithm is presented in §4, ML-based SA-SM is introduced in §5 and the results are given in §6. Finally, the paper concludes in §7.

2. System model

A heterogeneous radio-optical network is considered that consists of a number of legitimate users (L) and eavesdroppers (E), as shown in figure 1; a similar model was considered in [45]. The eavesdroppers are located within the coverage area of both radio and optical transmissions. Since both technologies cannot interfere with one another, both technologies are used concurrently and the receivers are equipped with both RF and optical frontends. The source (S) estimates the CSI of the transmission links via pilot signals. Key management is performed by S, which has a pool of size $\mathcal{P}$ keys that it can use for its transmission. The choice of the key (i.e. key selection algorithm) varies based on whether the eavesdropper is assumed to be active or passive and it is done on a periodical basis; §4 is dedicated to detailing SA-SM's key selection algorithm. When an E is active, it shares its CSI with the centralized source S to receive the information, while when passive its CSI remains unknown, similar to the assumption used in [45]. Typically, for channel equalization, the user (whether legitimate or eavesdropper) must be aware of the instantaneous CSI of its receiving link. However, we also consider the case where E remains passive, as it presents a more realistic scenario.

Without the need for S to send the new key to L over the air, SA-SM's novelty comes in designing a receiver capable of estimating which specific key S chooses out of the pool. In other words, in conventional rekeying techniques either the new key is exchanged over the air between the source and the nodes or the keys are prestored on the nodes themselves. Both those approaches, as previously mentioned, have their downfalls. The former suffers from the vulnerability of the key being intercepted over the air and overhead, and the latter is time exhaustive because the nodes have to search for the correct key from the set of available keys to decrypt the information. It is important to note that link signature keying techniques also do not require the exchange of keys; however, these techniques can only be used when the channel is said to be uncorrelated [48]. In RF transmission, it is normally presumed that links parted by at least half of a wavelength fade independently, yet this statement does not hold in optical transmission. In OWC, the light source acts as a transmitter that emits optical radiations rather than RF waves [49]. The major differences between optical and RF waves can be listed as follows: light waves cannot penetrate walls, the radius of the coverage area of an optical access point (AP) is relatively small in comparison with RF and the received power from the optical AP is significantly affected by the reception angle and distance between the transmitter and the receiver [50]. Most optical communication systems adopt intensity modulation (IM) and direct detection (DD) of the optical carrier, which indicates that only the signal intensity is transmitted. This requires the signal to be real and unipolar for transmission, which in return confines the type of modulation scheme that can be used.

Inter-symbol interference (ISI) is a major source of high bit error rates at high transmission rates. For combating ISI and its high spectral efficiency, orthogonal frequency division multiplexing (OFDM) is considered as one of the most powerful modulation schemes. However, traditional complex-valued OFDM signals may not be applied in IM/DD-based systems. Instead, real-valued OFDM techniques are used as a substitute to allow its adoption in optical systems. DC-biased optical OFDM (DCO-OFDM) and asymmetrically clipped optical OFDM (ACO-OFDM) [51] are considered the two most eminent optical OFDM techniques. Because of its

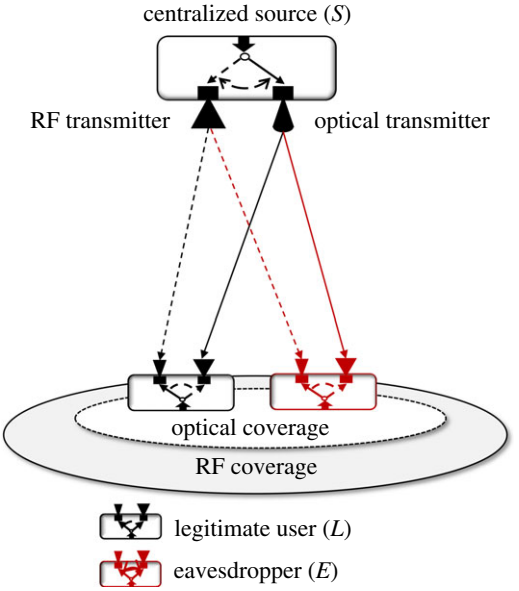

Figure 1. Heterogeneous radio-optical network showing, for simplicity, a single legitimate user, eavesdropper and the centralized source. As can be observed, all have both RF and optical frontends. (Online version in colour.)

tremendous advantages and wide adoption, SA-SM is based on traditional OFDM for the RF link and ACO-OFDM is used for the optical link owing to its high power efficiency. It is important to note that the channel in the optical domain is modelled by real-valued attenuation coefficients. Additionally, the signal incoming via the line-of-sight (LOS) path dominates those from the reflected paths. In fact, most OWC research focuses mainly on the LOS path and disregards multipath propagation. In this work, channel-enforced limitations are not our concentration area, thus our method is investigated in the presence of an additive white Gaussian noise (AWGN) channel for the optical link and a flat-fading Rayleigh model for RF.

An OFDM-transmitted signal after inverse fast Fourier transform (IFFT) with N sub-carriers can be expressed as [52]

$$x_{R/O}(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \mathbb{X}_n \, \mathrm{e}^{j2\pi(nk/N)}, \tag{2.1}$$

where X_n is the nth sub-carrier-modulated signal, k is the instantaneous time interval and the suffix R/O denotes the RF/optical link. In optical OFDM, Hermitian symmetry is applied on X_n before the IFFT operation to make $x_{R/O}(k)$ real. Furthermore, in ACO-OFDM systems only the odd subcarriers are used, and the residual subcarriers are nulled. Accordingly, the ACO-OFDM transmitted signal can be clipped at zero without loss of information. It is important to note that the differences between the RF and optical transmission are the frontends and the internal operation of the OFDM symbol generation. In conventional SM, extra bits are obtained from the spatial dimension. Even though spatial multiplexing, where parallel data streams are emitted from the transmitters, theoretically supplies the highest data rate among all MIMO methods, it necessitates low channel correlation, which is not the case in optical transmission. SM provides spectral efficiency gains, while relaxing the rigorous low channel correlation preconditions of spatial multiplexing by capturing additional bits from the spatial domain [53]. Moreover, SM's receiver architecture complexity is less than that spatial multiplexing, which is an important advantage. Given the potential of SM in RF-optical HetNets, SA-SM is proposed to address the confidentiality requirements of SM-based networks. However, the concept of SA-SM is versatile and can be applied to single-input single-output systems.

In conventional OFDM-based SM, the transmitted data are split by a data splitter into two divisions: $N \log_2 M$ bits and $\log_2 N_T$ bits, where N is the number of sub-carriers. M represents the modulation order of each subcarrier and N_T is the number of active transmitters. The $N \log_2 M$ bits are used to generate the OFDM symbol after the processes of modulation and IFFT, while the remaining $\log_2 N_T$ bits are used to choose which transmitting element will be active. On the other hand, in SA-SM, the centralized source controls the distribution of bits among the used technologies, i.e. RF and optical. Additionally, S modifies the OFDM symbol (generated from the $N \log_2 M$) based on the chosen key. The problem of optimizing the split of data among the used technologies is outside the scope of this work, as it has already been investigated in the literature [54]. Unlike our previous analysis in [47], we replace the legacy maximum-likelihood estimator with ML classification methods for key identification, which in return significantly reduces the computation time and allows a large number of keys to be used without the burden of the entailed computation time, as will be shown in §6.

3. The proposed security-aware spatial modulation technique

The security gain of SA-SM comes inherently and does not change the bit transmission period. In SA-SM, the time-domain signal is altered at the transmitter using an assigned PHY encryption key. This operation is analogous to implementing nonlinear masking of the data in the frequency domain. The concept of SA-SM can be observed to be similar to adding artificial noise (i.e. which is the key in our case); however, in SA-SM, the artificial noise can be estimated and removed by a legitimate receiver. The concept, however, should not also be confused with friendly jamming [55], as SA-SM does not require a separate jammer. The key that causes these alterations varies periodically and is assigned by the centralized source. The frequency of updating the keys can be as short as from one OFDM symbol to the other, i.e. the encryption key is different with every transmission, with a certain regular time interval based on the severity of the eavesdropping attacks. SA-SM can be used by both the RF and optical systems with the variation of the used frontends. Figure 2 presents the block diagram of the transmitter and receiver of an SA-SM system. As previously mentioned, the differences between RF and optical transmission are the used frontends and the OFDM symbol generation procedure. Yet, the method remains similar: replacing the employed ACO-OFDM for optical transmission by traditional OFDM for RF. Throughout the paper, including the figures, the superscript $(.)^N$ denotes an $N \times 1$ vector.

(a) Realization of security-aware spatial modulation's approach

The centralized source (based on the key selection algorithm) produces a key which is added to the original time-domain signal; hence, the key can be observed as an extra 'disguising' signal. The transmitted signal $s_{R/O}(k)$ can then be observed as a summation of two signals. The first signal, $x_{R/O}(k)$, is the OFDM time-domain signal, whether it is optical or RF, produced by a normalized M-QAM constellation whose energy is normalized to 1. The second signal (i.e. the key $p_{R/O}(k)$) is a binary pattern (i.e. with values equal to either 0 or 1). Given that SA-SM does not alter the frame structure of the transmitted symbol, conventional synchronization and channel estimation methods using preamble symbols can be used, such as the proposed work in [56] for the RF link and [57] for the optical link. Training symbol synchronization methods can also be used such as the work presented in [52]. Hence, the transmitted signal, $s_{R/O}$, becomes

$$s_{R/O}(k) = \beta x_{R/O}(k) + \alpha p_{R/O}(k), \tag{3.1}$$

where α and β are design parameters used to satisfy the security requirement and power constraints. The number of possible keys relies on a system parameter we denote as η, forming $\mathcal{P} = 2^\eta$ possible keys; the value of η must be a factor of N. In other words, the length of the key has to be equal to N, which is the IFFT length of the time-domain signal; a key is divided into η chucks, and each chunk has the same binary value. Given an example of a unipolar real OFDM for illustration, the effect of the system parameters α and η on SA-SM's transmitted signal is depicted

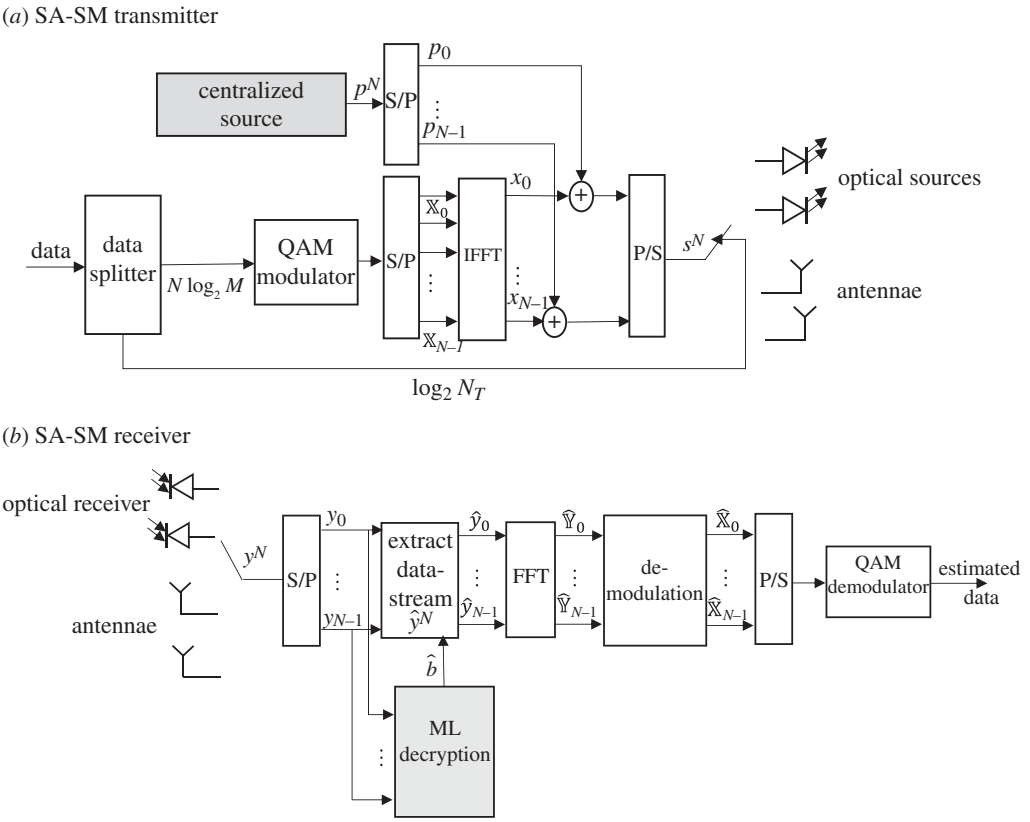

Figure 2. ML-based SA-SM transceiver with (*a*) a transmitter showing the centralized source providing the key to the transmitter and the data splitter responsible for controlling which transmitting elements are active, and (*b*) a receiver with the demodulation block entailing SM and QAM demodulation.

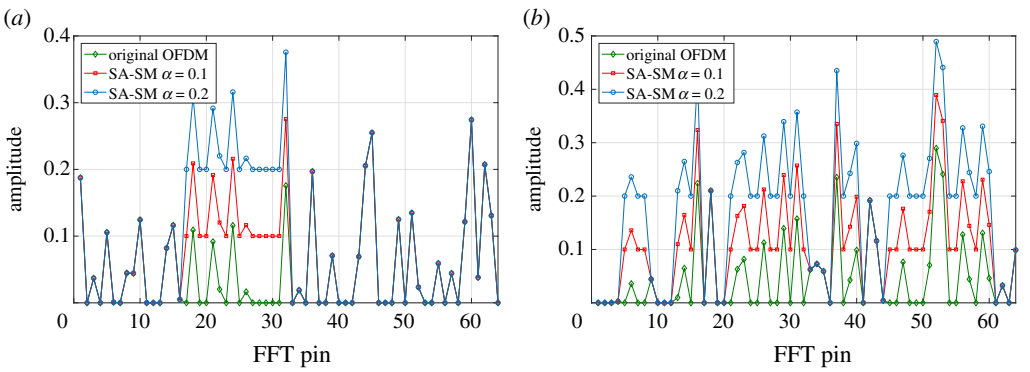

Figure 3. SA-SM transmitted signals showing the effect of system parameters α and η. For illustration, a unipolar real-valued ACO-OFDM signal with $N = 64$ is assumed and $\beta = 1$. (*a*) $\eta = 4$, (*b*) $\eta = 16$. (Online version in colour.)

in figure 3. The parameter α controls the amplitude of the transmitted signal chunks, while η controls the pattern of the chunks to which α is applied.

The information received at the legitimate receiver is indicated as

$$\begin{aligned} y_{L_{R/O}}(k) &= h_{L_{R/O}}(k)\, s_{R/O}(k) + n_{L_{R/O}}(k) \\ &= h_{L_{R/O}}(k)\Big[\beta x_{R/O}(k) + \alpha p_{R/O}(k)\Big] + n_{L_{R/O}}(k). \end{aligned} \tag{3.2}$$

Likewise, the information received by the eavesdropper E is

$$y_{E_{R/O}}(k) = h_{E_{R/O}}(k)\, s_{R/O}(k) + n_{E_{R/O}}(k)$$
$$= h_{E_{R/O}}(k)\Big[\beta x_{R/O}(k) + \alpha p_{R/O}(k)\Big] + n_{E_{R/O}}(k), \tag{3.3}$$

where $h_{L_{R/O}}$ and $h_{E_{R/O}}$ are the channel-fading coefficients of the legitimate and eavesdropper links, respectively. The parameters $n_{L_{R/O}}(k)$ and $n_{E_{R/O}}(k)$ are the zero mean AWGN random variables. For the eavesdropper, the signal quality is disturbed by the term $\alpha p_{R/O}(k)$, while the legitimate user (because it has prior knowledge of the key) does not suffer from this disturbance. It is important to note that the legitimate receiver has the ability to estimate the key $p_{R/O}(k)$, while the eavesdropper would have to attempt 2^N possible key combinations for every possible value of system parameter α per OFDM symbol. In most wireless standards, the number of OFDM subcarriers is at least 64, i.e. $N = 64$, which means that the eavesdropper would have 1.8×10^{19} versions of each OFDM symbol, assuming it had knowledge of α, without knowing which of these versions is the transmitted data. Readers are encouraged to refer to [47] for further details on the SA-SM technique.

The channel capacities of the legitimate and eavesdropper can be calculated as $C_{L_{R/O}} = \log_2(1 + \gamma_{L_{R/O}})$ and $C_{E_{R/O}} = \log_2(1 + \gamma_{E_{R/O}})$, respectively. The parameters $\gamma_{L_{R/O}}$ and $\gamma_{E_{R/O}}$ are the instantaneous SNRs of the L and E links, respectively. Owing to the disturbance factor, mentioned above, the SNR of L will be significantly higher than that of E. The secrecy capacity ($C_{s_{R/O}}$) can then be defined as

$$C_{s_{R/O}}(k) = \begin{cases} [C_{L_{R/O}}(k) - C_{E_{R/O}}(k)]^+, & \text{for } \gamma_{L_{R/O}} > \gamma_{E_{R/O}}, \\ 0, & \text{otherwise}, \end{cases} \tag{3.4}$$

where the superscript $[.]^+$ is denoted as a non-negative value, which entails that in order to achieve positive secrecy capacity $\gamma_{L_{R/O}}$ must be greater than $\gamma_{E_{R/O}}$.

(b) Secrecy capacity proposition

The average secrecy capacity of the RF link, denoted as $\overline{C}_{s_R}$, for a given instantaneous SNR of the L and E RF links, i.e. γ_{L_R} and γ_{E_R} respectively, can be defined as [58]

$$\overline{C}_{s_R}(\gamma_{L_R}, \gamma_{E_R}) = \mathbb{E}[C_{s_R}(k)] = \int_0^\infty \int_0^\infty C_s(k) f_{\gamma_{L_R}}(\gamma_{L_R}) f_{\gamma_{E_R}}(\gamma_{E_R}) d\gamma_{L_R}\, \mathrm{d}\gamma_{E_R}, \tag{3.5}$$

where $\mathbb{E}(.)$ is the expectation operation and $f_{\gamma_{L_R}}$ and $f_{\gamma_{E_R}}$ denote the probability density function (PDF) of γ_{L_R} and γ_{E_R}, respectively. Assuming a Nakagami-m fading distribution, the PDF of the received instantaneous SNR is given as

$$f_{\gamma_z}(\gamma) = \left(\frac{m}{\bar{\gamma}_z}\right)^m \frac{\gamma^{m-1}}{\Gamma(m)} \exp\left(-\frac{m\gamma}{\bar{\gamma}_z}\right), \quad \gamma \geq 0, \tag{3.6}$$

with m as the Nakagami fading parameter. It is important to note that the Rayleigh channel is considered a special case of the Nakagami-m fading distribution with $m = 1$ [59]. Then, the PDF can be simplified into

$$f_{\gamma_z}(\gamma) = \left(\frac{1}{\bar{\gamma}_z}\right) \frac{1}{\Gamma(1)} \exp\left(-\frac{\gamma}{\bar{\gamma}_z}\right), \quad \gamma \geq 0, \tag{3.7}$$

where $\Gamma(.)$ is denoted as the Gamma function [60] and $\bar{\gamma}_z$ is the average instantaneous SNR defined as

$$\bar{\gamma}_z = \frac{P_s \mathbb{E}(|h_z|^2)}{N_z}, \tag{3.8}$$

where P_s is the transmitted power from source S and N_z is the AWGN spectral density. After some algebraic manipulation, (3.5) can be rewritten as

$$\overline{C}_{s_R}(\gamma_{L_R}, \gamma_{E_R}) = \frac{1}{\ln 2}\left[\sum_{g=1}^{\infty}(-1)^{g-1} \frac{g}{\Gamma(1)}\left(\overline{C}_1 - \frac{1}{\Gamma(1)}\overline{C}_2\right)\right]. \tag{3.9}$$

The terms $\overline{C}_1$ and $\overline{C}_2$, using the Meijer-G function denoted as $G(.)$, are given as

$$\overline{C}_1 = \frac{\Gamma(1+g)\Gamma(-g)}{\Gamma(1-g)} \tag{3.10}$$

and

$$\overline{C}_2 = \frac{1}{\bar{\gamma}_{E_R}}^{-g} G_{3,3}^{2,2}\left(\frac{\gamma_{E_R}}{\gamma_{L_R}}\Big|_{1,-g,0}^{1,-g,1/g}\right). \tag{3.11}$$

The average secrecy capacity of the optical link can be expressed similarly to the RF link with the variation that the instantaneous SNR is limited to a range controlled by the optical transmitter/receiver alignment. Thus, the optical average secrecy capacity can be expressed as

$$\overline{C}_{s_O}(\gamma_{L_O}, \gamma_{E_O}) = \mathbb{E}[C_{s_O}(k)] = \int_{\gamma_{\min}}^{\gamma_{\max}} \int_{\gamma_{\min}}^{\gamma_{\max}} C_s(k) f_{\gamma_{L_O}}(\gamma_{L_O}) f_{\gamma_{E_O}}(\gamma_{E_O})\, \mathrm{d}\gamma_{L_O} d\gamma_{E_O}. \tag{3.12}$$

Assuming a Lambertian radiation pattern with an order $l = -1/\log_2(\cos(\phi_{1/2}))$, with $\phi_{1/2}$ the semiangle of the optical transmitter, (3.12) can be expressed as

$$\overline{C}_{s_O}(\gamma_{L_O}, \gamma_{E_O}) = \frac{1}{\ln 2}\left[v(1-v)\overline{C}_3 + K\left(\frac{2v}{\bar{\gamma}_{L_O}^{-(1/(l+3))}} - \frac{1}{\bar{\gamma}_{E_O}^{-(1/(l+3))}}\right)\overline{C}_4 - \frac{K^2}{(\bar{\gamma}_{L_O}, \bar{\gamma}_{E_O})^{-(1/(l+3))}}\overline{C}_5\right], \tag{3.13}$$

where $v = (1 + (L^2/r^2))$ with L is the vertical distance from the source to the optical receiver and r is the radius of the optical coverage. The parameters $\overline{C}_3$, $\overline{C}_4$ and $\overline{C}_5$ are

$$\overline{C}_3 = \sum_{g=1}^{\infty}(-1)^{g-1}[\gamma_{\max}^g - \gamma_{\min}^g], \tag{3.14}$$

$$\overline{C}_4 = \sum_{g=1}^{\infty}(-1)^{g-1} g\left[\frac{\gamma_{\max}^{g-\frac{1}{l+3}} - \gamma_{\min}^{g-(1/(l+3))}}{g-(1/(l+3))}\right] \tag{3.15}$$

and

$$\overline{C}_5 = \sum_{g=1}^{\infty}(-1)^{g-1} g\left[\frac{\gamma_{\max}^{g-(2/(l+3))} - \gamma_{\min}^{g-(2/(l+3))}}{g-(2/(l+3))}\right]. \tag{3.16}$$

For simplicity, by ignoring the presence of an optical filter and an optical concentrator, $\gamma_{\min}$ and $\gamma_{\max}$ are expressed as

$$\gamma_{\min} = \frac{\varepsilon^2 P_s^2}{N_z B}\frac{1}{4\pi^2} A^2 R^2 \frac{\left((l+1)L^{l+1}\right)^2}{L^{2(l+3)}} \tag{3.17}$$

and

$$\gamma_{\max} = \frac{\varepsilon^2 P_s^2}{N_z B}\frac{1}{4\pi^2} A^2 R^2 \frac{\left((l+1)L^{l+1}\right)^2}{(r^2+L^2)^{l+3}}, \tag{3.18}$$

where ε is the electrical to optical efficiency, B is the bandwidth, A is the detector area and R is the responsivity.

4. Key selection algorithm

As previously mentioned, in the proposed system model, the radio and optical technologies can be used concurrently. The transmitters remain connected to the legitimate receivers as long as the secrecy rate remains positive. However, when the secrecy rate of any technology (i.e. RF or optical) drops below a certain threshold, C_s^{th}, that entails that the key has been compromised and the source (depicted in figure 1) chooses another key from the pool and uses it. C_s^{th} is a preset value which has a minimum of 0, and its value depends on the security requirements of the system. If

C_s cannot be calculated, because $\gamma_{E_{R/O}}$ is unavailable, then the algorithm switches to random key selection. Let us consider a binary decision indicator (I_{p_i}) for each key $p_i \in \mathcal{P}$, as follows:

$$I_{p_i} = \begin{cases} 1, & \text{if key } p_i \text{ is available,} \\ 0, & \text{otherwise.} \end{cases}$$

Our channel assignment algorithm functions as follows.

— The keys that are already assigned to other legitimate users and those that have been compromised will be eliminated from $\mathcal{P}$, producing a new set of feasible keys $\mathcal{P}^f$. Each key has its own binary decision indicator, with 1 meaning it is available for use and 0 meaning either it is temporarily unavailable or has been leaked. A set of length $\mathcal{P}$, I_p, contains the binary indicators for all the keys.
— Using $\gamma_{L_{R/O}}$ and $\gamma_{E_{R/O}}$, the algorithm calculates C_s using all available keys in $\mathcal{P}^f$, the calculated C_s using key i is denoted as $C_s^{(i)}$. If C_s falls below the threshold or cannot be calculated, then the corresponding key is omitted from the feasible key pool obtained in the previous step.
— If the algorithm fails to find a solution, i.e. C_s cannot be computed for all available keys, it switches to random key selection out of the keys that are available based on the original I_p inputted to the algorithm. The random chosen key is denoted as p^* and its corresponding indicator is changed to zero to mark that it has been assigned and I_p is updated accordingly.
— If a solution can be found, the algorithm chooses the key with the highest secrecy capacity. Similar to the previous step, the key's corresponding indicator is changed to zero to mark that it has been assigned and I_p is updated accordingly.

Algorithm 1 shows the pseudocode of the SA-SM key selection algorithm.

Algorithm 1. SA-SM key assignment.

Input: $\mathcal{P}$, I_p, $\gamma_{L_{R/O}}$, $\gamma_{E_{R/O}}$, C_s^{th}
Output: An available key p
Let $\mathcal{P}^f = I_p \times \mathcal{P}$
for all $i \in \mathcal{P}^f$
  Compute $C_s^{(i)}$ using (3.4)
  if $C_s^{(i)} < C_s^{th}$ **or** $C_s^{(i)} = \phi$
    $\mathcal{P}^f = \mathcal{P}^f - \{i\}$
  end-of-if
end-of-for
if $\mathcal{P}^f = \phi$
  Random selection of $p^* \in (I_p \times \mathcal{P})$
  Adjust the key indicator $I_p^* = 0$
  Return p_i and updated I_p
else
  for all $i \in \mathcal{P}^f$
    Sort the keys in an increasing order of $C_s^{(i)}$
  end-of-for
  Let $\mathcal{U}$ be the sorted key list
  Identify the key that is on the top of $\mathcal{U}$
  Return p_i and updated I_p
end-of-if

5. Reception of SA-SM signal

(a) Classical approach

The classical approach for SA-SM's detection, which is the analysis in [47], starts by invoking maximum-likelihood detection (MLD) on the received time-domain signal to estimate the key, followed by frequency-domain demodulation of the SM-based signal. The first stage of SA-SM's demodulation process can be outlined as hypothesis testing with nuisance parameters, based on $\mathcal{P}$ hypotheses indicated as $\mathcal{H}_j$, where $j = 1, \ldots, \mathcal{P}$, equivalent to the keys conditioned as a vector $p^N_{\mathcal{H}_j}$. The auxiliary vectors, $u^N_{\mathcal{H}_j}$, given by $u^N_{\mathcal{H}_j} = y^N - (\Psi/2)p^N_{\mathcal{H}_j}$ are constructed, with y^N representing the received time-domain OFDM signal. The MLD chooses the hypothesis that maximizes the likelihood function of the estimated binary sequence, $\hat{b}$, i.e.

$$\begin{aligned}\hat{b} &= \arg\max_j \left[f_{u_{\mathcal{H}_j}}(u_{0,\mathcal{H}_j}, \ldots, u_{N-1,\mathcal{H}_j} | \hat{s}_{\mathcal{H}_j}, \mathcal{H}_j) \right] \\ &= \arg\min_j \sum_{n=0}^{N-1} (u_{n,\mathcal{H}_j} - \hat{s}_{n,\mathcal{H}_j})^2 \end{aligned} \tag{5.1}$$

with $f_{u_{\mathcal{H}_j}}$ presenting the PDF of $u_{\mathcal{H}_j}$. When the key is estimated, and using simple mathematical manipulations based on equation (3.1), an estimate of x_N is calculated, i.e. $\hat{x}^N = (1/\beta)u^N_{\mathcal{H}_j}$. The output is then converted to the frequency domain to estimate the SM-based symbols. For the second stage in detection, which is the demodulation of OFDM SM-based signals, there are multiple solutions proposed in the literature, including using maximum receive ratio combining (MRRC) on each sub-carrier to estimate the transmitting element index presented in [61] and iterative maximum-likelihood-based receivers such as [62]. The evaluation in §6 adopts the MRRC approach in [61].

Based on equation (3.1) and as depicted in figure 2*a*, SA-SM signal generation requires two extra multiplication operations. Thus, for an N-length optical OFDM symbol, the SA-SM transmitter's complexity increases by $2N$ operations. Similarly, at the receiver's side, the system complexity increases. However, the receiver's complexity increases further based on the parameters $\mathcal{P}$. SA-SM's maximum-likelihood-based receiver would require, per hypothesis (there are $\mathcal{P}$ hypotheses), N multiplications to calculate the auxiliary vectors ($u^N_{\mathcal{H}_j}$), N multiplications for the binary sequences estimates ($\hat{b}$) and N for the transmitted symbol estimation ($\hat{x}^N$). In this work, we are using the same definitions as defined in [63]; the number of evaluations an algorithm performs to reach a solution is defined as the order of complexity, and the number of real-valued multiplications for solving the problem is the computational complexity. Based on these definitions, SA-SM's maximum likelihood receiver's computational complexity is increased by a factor of $3N\mathcal{P}$, while its order of complexity is increased by $\mathcal{P}$. In order to increase the security of the system and adopt a large number of keys ($\mathcal{P}$), alternative detectors are needed to reduce the entailed complexity.

(b) Machine learning-based security-aware spatial modulation

As the key estimation problem can be perceived as a classification problem, ML-based classifiers are proposed to substitute the previously discussed classical approach. The chosen ML-based classifiers are an SVM, a multi-nominal LR and an NN. We intentionally use well-known multi-class classification approaches which are readily available off-the-shelf as hardware components that can be employed in practice. The ML decryption block highlighted in figure 2*b* consists of one of the aforementioned modules. The modules are trained offline with the supervised dataset then added to the receivers after testing and validation. ML algorithms are normally considered as techniques that require intensive computational complexity. However, in reality, the training phase of the algorithms is the hindrance and not the prediction phase. Since the set of possible

keys that can be applied are predetermined, the ML classifiers can be trained offline. Hence, system complexity evaluation can discard training complexity.

(i) Support vector machines

SVMs are supervised techniques used for classification, outliner detection and regression. An SVM initially builds a hyper-plane, or a set of hyper-planes, in a high (maybe even infinite)-dimensional space by mapping the provided training dataset using a nonlinear feature-mapping function $\phi(d)$, where d is the training data [64]. Afterwards, an optimization method is applied that aims to find the maximum separation margin between the classes lying in the feature space and minimize the training error ξ_z. Given a set of training data (d_z, c_z), $z = 1, \ldots, Z$, where $c_z \in \{-1, 1\}$ denote the labels of the training d_z; -1 entails not belonging to the class and 1 entails belonging to the class. The optimization problem is conveyed as

$$\begin{aligned} &\text{minimize}: J_{SVM} = \frac{1}{2} \parallel \omega \parallel^2 + D \sum_{z=1}^{Z} \xi_z \\ &\text{subject to}: c_z\left(\omega \cdot \phi(d_z) + b\right) \geq 1 - \xi_z, \quad z = 1, \ldots, Z, \\ &\quad \xi_z \geq 0, \quad z = 1, \ldots, Z, \end{aligned} \tag{5.2}$$

where D is a parameter specified by the programmer and controls the trade-off between the minimizing training error and maximizing the distance of the separating margins; in our implementation $D = 1$. The parameter b is a bias parameter and ω represents the weights. Another form of the SVM problem can be given by

$$\min_{\omega} \frac{1}{2}\omega^T\omega + D \sum_{z=1}^{Z} \xi(\omega, d_z, c_z), \tag{5.3}$$

where $(.)^T$ denotes the transpose operation. For multiclass classification applications, as in our application, two methods are normally used for SVM realization; one-against-all (i.e. one-versus-all) and one-against-one (i.e. one-versus-one). One-versus-all forms an array of SVMs (equivalent to the number of classes). In our implementation, there are $\mathcal{P}$ classes. Each sample in the ith class is trained with positive labels for the ith SVM, the rest of the $\mathcal{P} - 1$ classes are negatively labelled. In one-versus-one, $\mathcal{P}(\mathcal{P} - 1)/2$ SVMs are trained using samples belonging to two classes only. In this work, the SVM multi-class support follows a one-versus-one scheme. The implementation is based on the popular SVM library LIBSVM [65].

(ii) Logistic regression

Despite its name, LR is a linear model used for classification and not regression. The cross-entropy loss function, which measures the difference between the actual and estimated distribution, is the mostly applied objective function for training LR. The same problem given in (5.3) needs to be solved for LR with the exception of the loss function, $\xi(\omega, d_z, c_z)$, which is now $\log(1 + e^{-c_z(\omega^T d_z + b)})$ for L2-regularized LR. The objective is also to calculate the set of weights and biases that minimizes this loss function. Hence, the optimization problem can be formulated as

$$\min_{\omega, b} \frac{1}{2}\omega^T\omega + D \sum_{z=1}^{Z} \log(1 + e^{-c_z(\omega^T d_z + b)}). \tag{5.4}$$

Multiple solvers can be used to solve this optimization problem, including the lbfgs solver. It is a limited-memory quasi-Newton code for bound-constrained optimization that approximates the Broyden–Fletcher–Goldfarb–Shanno algorithm. Multi-nomial LR is a simple extension of the aforementioned binary LR to allow more than two classes. Like binary LR, multi-nomial LR uses the maximum-likelihood principle to calculate categorical membership probability. Using the

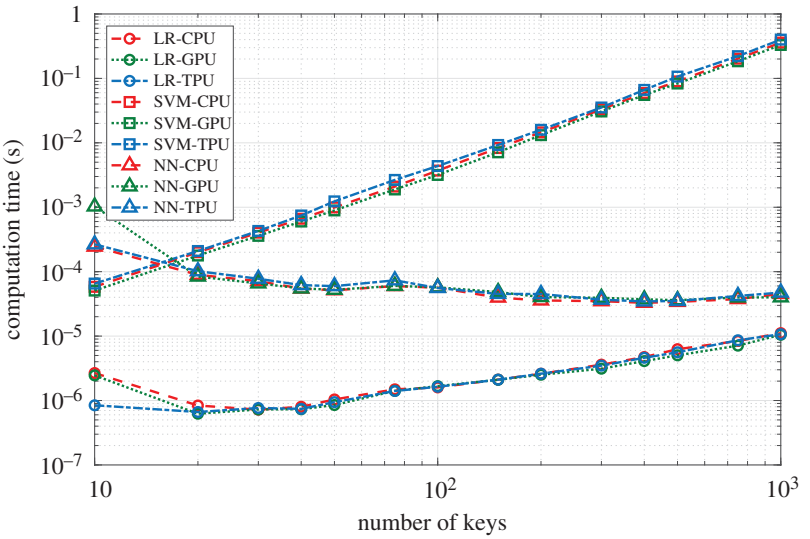

Figure 4. Computation times of the three ML algorithms using various hardware architectures. (Online version in colour.)

training samples, a model is trained to associate the input to a class. In this work, a multi-nomial LR with L2 regularization is trained using the lbfgs solver, which is chosen for its robustness.

(iii) Neural network

An NN is formed of small computing units, where each unit takes a vector of input values and creates a single output value and learns to instigate features as part of the task of learning to classify; NNs share much of the same mathematics as LR. In our implementation, in order to reserve the complexity of the system, we train a supervised feed-forward fully-connected NN formed by a single hidden layer. A feed-forward network can be defined as a network where the computing units are connected without cycles, i.e. each layer passes its output to the next higher layer without any outputs returned back to lower layers. Fully connected means that each computing unit receives the outputs from all the units in the layer preceding it. Our NN is composed of an input layer and a single hidden layer (made up of 50 neurons) followed by a dense layer with a softmax activation function for classification. The training aims to minimize the sparse categorical cross-entropy loss function, which can be defined as

$$J(\omega) = \frac{-1}{\mathcal{P}} \sum_{i=1}^{\mathcal{P}} \Big[p_i \log(\hat{p}_i) + (1 - p_i) \log(1 - \hat{p}_i) \Big], \tag{5.5}$$

where ω are the weights of the NN, p_i is the true key and $\hat{p}_i$ is the predicted key. The training data are formed of $(250 \times \mathcal{P})$ frames, which constitute the sample size. The data are split with a ratio of 8 : 2 for training and testing, respectively. The NN is trained for 10 epochs using a single SNR value equal to 10 dB. The number of trainable parameters of this NN is equal to $(S_H\mathcal{P} + \mathcal{P}) + (NS_H + S_H)$, where S_H denotes the number of neurons in the hidden layer. Since the depth of an NN and the number of nodes in its hidden layers determine its complexity, the architecture of the proposed NN is limited to a single hidden layer in order to reduce its computation complexity and keep the number of trainable parameters to a minimum.

6. Results and analysis

We used Google's colab environment to employ the different hardware architectures provided by Google for performance comparison. The hardware architectures include CPUs, TPUs and GPUs.

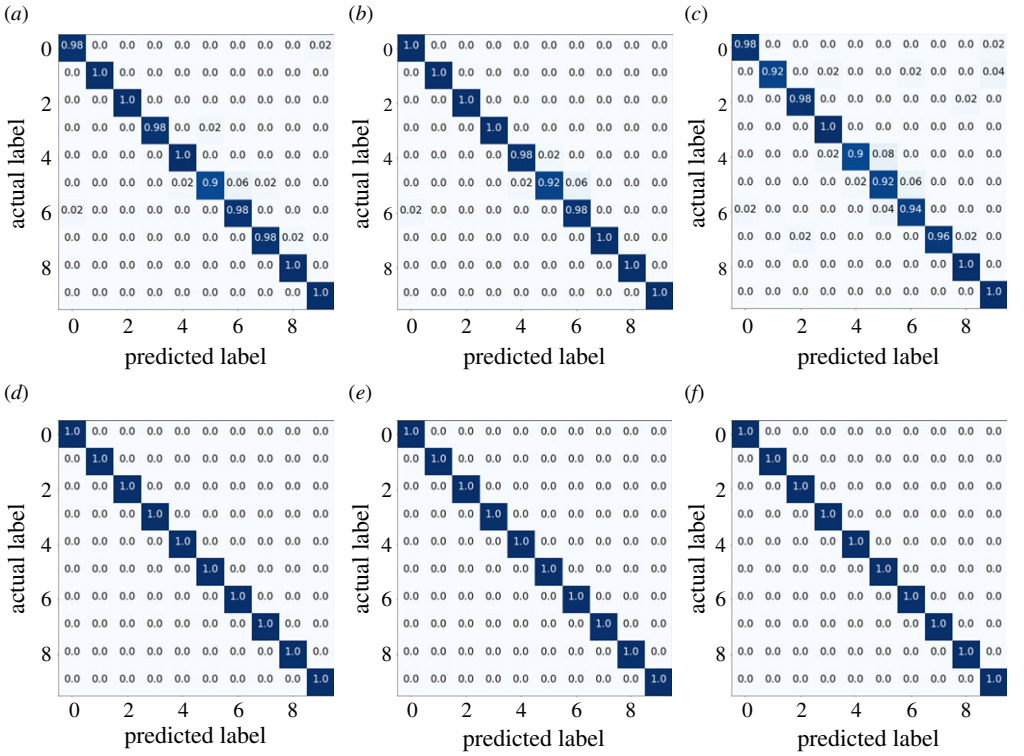

Figure 5. Confusion matrices for the different ML methods for $\mathcal{P} = 10$ and $\eta = 16$, where $\alpha = 0.1$ in (*a–c*) and $\alpha = 0.2$ in (*d–f*). (*a*) Linear kernel SVM, (*b*) LR with an lbfgs solver, (*c*) one-layer NN, (*d*) linear kernel SVM, (*e*) LR with an lbfgs solver, (*f*) one-layer NN. (Online version in colour.)

Firstly, the computation time required for the ML techniques to estimate the PHY encryption key using the various hardware architectures versus the number of keys is calculated and shown in figure 4. As shown, the SVM's performance was the worst by having the highest computation times. On the other hand, both the NN and the LR are able to classify in less than 10^{-4} s for $\mathcal{P} = 1000$. However, the NN's computation time remained relatively constant and independent of the number of keys, which makes the NN's performance more predictable and consistent than those of LR and SVM. Another observation is that the variation among the different architectures is minimal; yet, the TPU is considered the best in terms of computation time performance. Then, the key estimation accuracy of the proposed ML techniques is evaluated. The confusion matrices for the various ML techniques are depicted in figure 5, with $\mathcal{P} = 10$ at system parameter $\alpha = 0.1$ and 0.2 with $\eta = 16$ and $\beta = 1$. As can be observed, all the ML techniques precisely estimate the encryption key with a 100% classification accuracy at $\alpha = 0.2$; however, at $\alpha = 0.1$ mislabelling occurs. At $\alpha = 0.1$, the SVM has the best identification accuracy with seven keys correctly identified and only three mislabelled with a minimum accuracy of 92%. The LR, on the other hand, labelled five correctly with a minimum accuracy of 90%, and the NN mislabelled five also with a minimum accuracy of 90%. Figure 6 gives a more thorough insight into the accuracy of the proposed ML by measuring the classification accuracy versus the number of keys ($\mathcal{P}$) for two values of the system parameter η. In line with the results in figure 5, the identification accuracy is consistently better at $\alpha = 0.2$ for both $\eta = 16$ and $\eta = 32$. Intuitively, as the number of keys increases, the accuracy decreases. Accuracy also seems to improve significantly by increasing η, yielding a minimum accuracy of 85% at $\alpha = 0.1$ (the NN), which is a notable improvement over the 72% accuracy at $\alpha = 0.1$ for $\mathcal{P} = 1000$. Even though the NN seems to have the lowest accuracy, at $\alpha = 0.1$ and $\eta = 32$, as shown

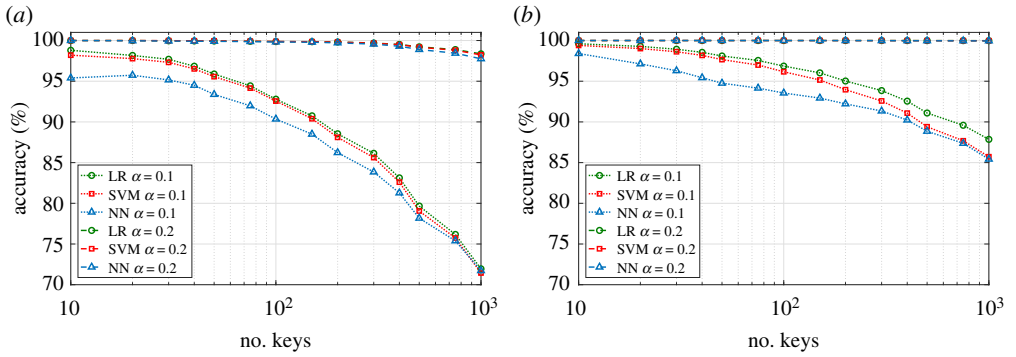

Figure 6. Key estimation accuracy of the proposed ML techniques versus number of keys given two values of the SA-SM's system design parameters, α and η. (*a*) $\eta = 16$, (*b*) $\eta = 32$. (Online version in colour.)

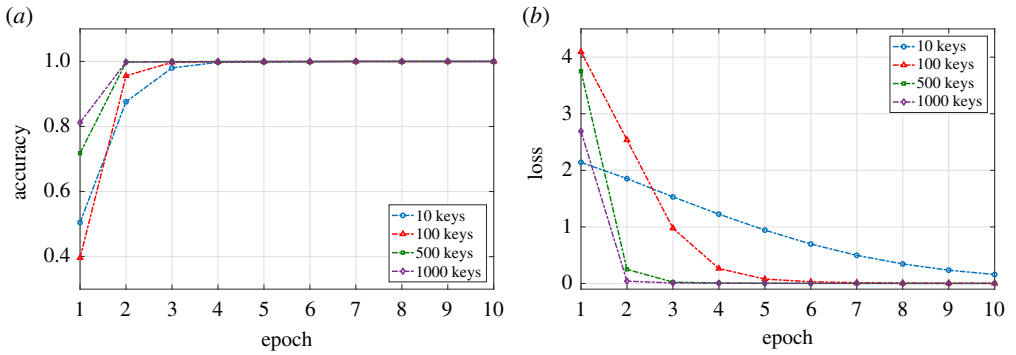

Figure 7. The NN's accuracy and loss while training versus the number of training epochs for various $\mathcal{P}$ values. (*a*) Training accuracy, (*b*) training loss. (Online version in colour.)

in figure 6*b*, all the techniques are capable of estimating the encryption key with about 100% accuracy at $\alpha = 0.2$. Given our findings and the fact that the computation time of the NN remains relatively constant irrespective of the number of keys used, the NN is chosen with $\alpha = 0.2$ and $\eta = 32$ for the remainder of the analysis. To get a better understanding of the performance of the NN while training, the training accuracy and loss versus number of epochs is presented in figure 7. As can be seen in figure 7*a*, only four epochs are needed for the NN to reach a 100% accuracy for various values of $\mathcal{P}$. As previously mentioned, the size of the dataset used to train the NN is $0.8 \times 250 \times \mathcal{P}$; in other words, in the case of $\mathcal{P} = 1000$ the NN is trained using 200 000 frames. Because the training data increase with the number of keys, the NN reaches 100% accuracy and the loss drops to 0 faster as the number of keys increases. The anomaly is the behaviour of the NN at $\mathcal{P} = 10$, where the loss approaches (but does not reach) 0 yet the accuracy is 100% and the confusion matrix (figure 5*f*) shows no mislabelling. Because of this anomaly, we set the number of epochs to allow the NN to converge. It is important to note that the perception of SA-SM is scalable: as previously mentioned, the number of keys that can be used is equal to 2^{η}, i.e. at $\eta = 32$ the system can accommodate over 4×10^9 different keys. However, in our analysis, we set $\mathcal{P} = 1000$ as an example value to show the potential of SA-SM.

To test the security gain of SA-SM, the worst-case scenario, which is the case of unknown C_s, is evaluated and the algorithm is performed prior to each transmission, i.e. the key is changed with each frame. The secrecy bit-error-rate (BER), which can be defined as the BER of the eavesdropper, is firstly tested for the optical link under the AWGN channel model in figure 8*a*

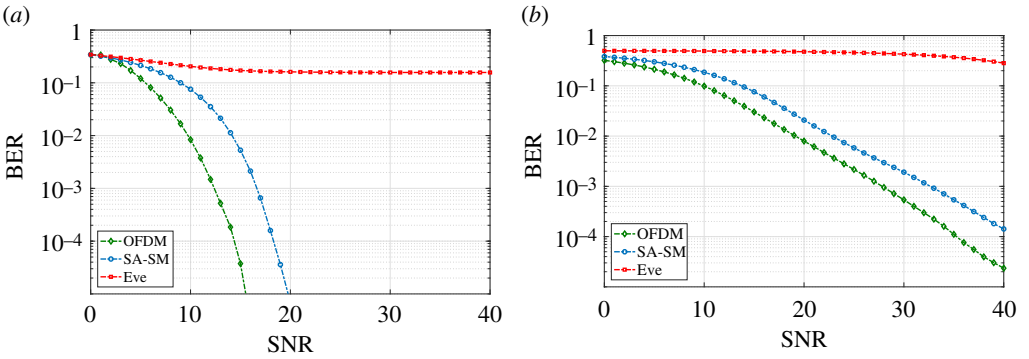

Figure 8. NN-based SA-SM BER performance versus SNR, depicting the legitimate user (SA-SM) BER in comparison with that of the eavesdropper (Eve) for 16-QAM OFDM transmission with $N = 64$, $\eta = 32$, $\alpha = 0.2$ and $\mathcal{P} = 1000$. (*a*) Optical link under AWGN, (*b*) RF link under flat-fading Rayleigh. (Online version in colour.)

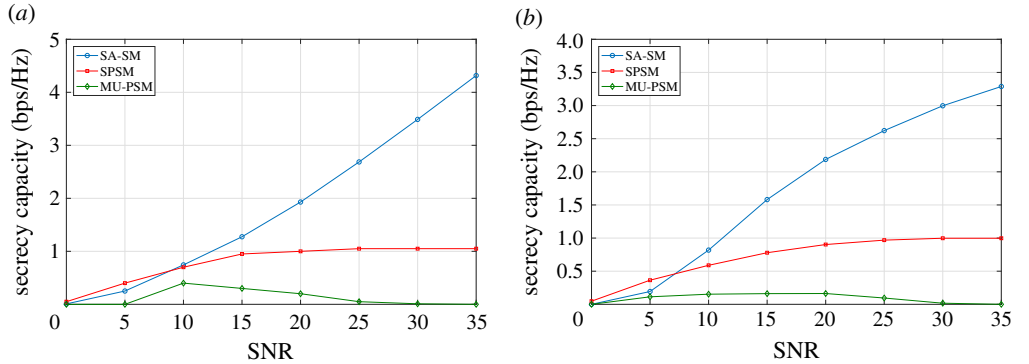

Figure 9. Secrecy capacity, C_s, for the optical link in (*a*) and for the RF link in (*b*) at $\alpha = 0.2$, 16-QAM OFDM transmission, $\eta = 32$, $\beta = 1$ and $\mathcal{P} = 1000$. As can be observed, NN-based SA-SM causes C_s to always maintain a positive value. (*a*) Optical link, (*b*) RF link. (Online version in colour.)

and for the RF transmission under the flat-fading Rayleigh channel model in figure 8*b* for NN-based SA-SM. In both technologies, the eavesdropper's BER remains under 10^{-1} and for the RF it remains relatively stable at 0.5, which is equivalent to random guessing. The eavesdropper's BER is annotated as Eve and is depicted in red in the coloured online version. It is important to highlight that the reason why the secrecy BER is higher in RF than in the optical link is because of channel impairments and not the SA-SM technique. To show the effect of parameter α, the transmitted signal is normalized (has a maximum of 1). At $\alpha = 0.2$, the eavesdropper's BER saturates within the range of 10^{-1} with a minimal SNR penalty of about 5 dB between the SA-SM signal and conventional OFDM transmission. Increasing α causes an increase in the SNR penalty; however, the higher the α the higher the identification accuracy. Since $\alpha = 0.2$ provides 100% accuracy even at $\mathcal{P} = 1000$, we do not include higher values of α in our analysis. Yet, we anticipate that, in applications that require more than 1000 keys, a higher value of α would be needed. The secrecy capacity of SA-SM is also investigated and provided in figure 9. The performance of SA-SM is compared with the jamming scheme proposed in [35], multi-user precoding-aided spatial modulation (MU-PSM) and the precoding plus jamming scheme proposed in [30] and secret precoding-aided spatial modulation (SPSM). In our comparison, the eavesdropper is assumed to have six receiving elements. As can be observed, SA-SM's secrecy capacity outperforms MU-PSM and SPSM, which suffer from the eavesdropper having multiple

receiving elements. SA-SM's performance, on the other hand, remains positive and is inherently proportional to SNR. SA-SM's perception allows its secrecy capacity to be reserved regardless of the number of receiving elements the eavesdropper has, causing SA-SM's superiority in terms of secrecy capacity performance. It can be noted that the secrecy capacity in the optical link is higher than that in the RF; however, again, it is due to the severity of channel impairment in RF in comparison with the AWGN model for optical.

7. Conclusion

SA-SM is introduced as a PLS technique for multi-technology MIMO-based radio-optical HetNets. The analysis includes a scalable key generation algorithm that allows periodical rekeying to protect the system from eavesdropping attacks without the need for exchanging the keys over the air or storing them on the communicating nodes. SA-SM's key selection algorithm chooses the key that maximizes the secrecy rate of the system when the eavesdropper's CSI is known. However, if the eavesdropper's CSI is unknown, it switches to random key assignment. The rate at which the key is changed can be minimized to a frame basis, which serves in impeding the eavesdropper from decrypting the information. SA-SM's realization uses simple and off-the-shelf ML algorithms for key identification and classification, which makes SA-SM suitable for multiple applications including IoT-based systems. Additionally, our execution is implemented using various hardware architectures, including GPUs, CPUs and TPUs, to satisfy various nodes' realizations and capabilities. The performances of the proposed ML techniques, namely SVM, LR and a single-layer NN, are compared in terms of classification accuracy and computation time. The secrecy gain of SA-SM is evaluated using two metrics: eavesdropper's BER and secrecy capacity for both the RF and optical transmissions. Results show that the eavesdropper's BER can be maintained below 10^{-1} for the optical and RF transmissions, even in the case where the eavesdropper's CSI is unknown by switching between 1000 PHY encrpytion keys, while introducing a minimal SNR penalty which is less than 5 dB. The secrecy capacity of SA-SM is also evaluated and is shown to maintain a positive value that is proportional to the system's SNR value; results show that about 2 bps/Hz secrecy capacity gain can be achieved at an SNR value of 20 dB for 16-QAM transmission.

Data accessibility. The codes used to create the dataset, train the ML algorithms and analyse the data can be accessed at https://github.com/ounety/ML-SASM to be reused under the CC BY licence. For more details, see https://creativecommmons.org/licenses/by/4.0/.

Authors' contributions. All authors contributed to the analysis and writing of the manuscript, tested the code and gave final approval for publication.

Competing interests. We declare we have no competing interests.

Funding. The authors are grateful for partial support by the National Science Foundation (NSF) under grant no. ECCS-1331018 and the Engineering Research Centers Program of the NSF under NSF Cooperative Agreement no. EEC-0812056.

Acknowledgements. The authors would like to sincerely thank the board member and referees whose comments helped improve and clarify this manuscript.

References

1. Jiang C, Zhang H, Ren Y, Han Z, Chen K, Hanzo L. 2017 Machine learning paradigms for next-generation wireless networks. *IEEE Wirel. Commun.* **24**, 98–105. (doi:10.1109/MWC.2016.1500356WC)
2. Zou Y, Zhu J, Wang X, Hanzo L. 2016 A survey on wireless security: technical challenges, recent advances, and future trends. *Proc. IEEE* **104**, 1727–1765. (doi:10.1109/JPROC.2016.2558521)
3. Shiu Y, Chang SY, Wu H, Huang SC, Chen H. 2011 Physical layer security in wireless networks: a tutorial. *IEEE Wirel. Commun.* **18**, 66–74. (doi:10.1109/MWC.2011.5751298)

4. Ma J, Shrestha R, Adelberg J, Yeh CY, Hossain Z, Knightly E, Jornet JM, Mittleman DM. 2018 Security and eavesdropping in terahertz wireless links. *Nature* **563**, 89–95. (doi:10.1038/s41586-018-0609-x)
5. Ye H, Li GY, Juang B. 2018 Power of deep learning for channel estimation and signal detection in OFDM systems. *IEEE Wirel. Commun. Lett.* **7**, 114–117. (doi:10.1109/LWC.2017.2757490)
6. Samuel N, Diskin T, Wiesel A. 2017 Deep MIMO detection. In *Proc. 2017 IEEE 18th Int. Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Sapporo, Japan, 3–6 July 2017*, pp. 1–5. Piscataway, NJ: IEEE Signal Processing Society.
7. Farsad N, Goldsmith A. 2018 Neural network detection of data sequences in communication systems. *IEEE Trans. Signal Process.* **66**, 5663–5678. (doi:10.1109/TSP.2018.2868322)
8. He H, Wen C, Jin S, Li GY. 2018 Deep learning-based channel estimation for beamspace mmWave massive MIMO systems. *IEEE Wirel. Commun. Lett.* **7**, 852–855. (doi:10.1109/LWC.2018.2832128)
9. Neumann D, Wiese T, Utschick W. 2018 Learning the MMSE channel estimator. *IEEE Trans. Signal Process.* **66**, 2905–2917. (doi:10.1109/TSP.2018.2838577)
10. Farsad N, Rao M, Goldsmith A. 2018 Deep learning for joint source-channel coding of text. In *Proc. of the 2018 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), Calgary, Canada, 15–20 April 2018*, pp. 2326–2330. Piscataway, NJ: IEEE Signal Processing Society.
11. Nachmani E, Marciano E, Lugosch L, Gross WJ, Burshtein D, Be'ery Y. 2018 Deep learning methods for improved decoding of linear codes. *IEEE J. Sel. Top. Signal Process.* **12**, 119–131. (doi:10.1109/JSTSP.2017.2788405)
12. Gruber T, Cammerer S, Hoydis J, Brink St. 2017 On deep learning-based channel decoding. In *Proc. 2017 51st Annu. Conf. on Information Sciences and Systems (CISS), Baltimore, MD, 22–24 March 2017*, pp. 1–6.
13. Wen C, Shih W, Jin S. 2018 Deep learning for massive MIMO CSI feedback. *IEEE Wirel. Commun. Lett.* **7**, 748–751. (doi:10.1109/LWC.2018.2818160)
14. Wyner AD. 1975 The wire-tap channel. *Bell Syst. Tech. J.* **54**, 1355–1387. (doi:10.1002/j.1538-7305.1975.tb02040.x)
15. Leung-Yan-Cheong S, Hellman M. 1978 The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **24**, 451–456. (doi:10.1109/TIT.1978.1055917)
16. Ng DWK, Lo ES, Schober R. 2014 Robust beamforming for secure communication in systems with wireless information and power transfer. *IEEE Trans. Wirel. Commun.* **13**, 4599–4615. (doi:10.1109/TWC.2014.2314654)
17. Liao W, Chang T, Ma W, Chi C. 2011 QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach. *IEEE Trans. Signal Process.* **59**, 1202–1216. (doi:10.1109/TSP.2010.2094610)
18. Lin P, Lai S, Lin S, Su H. 2013 On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels. *IEEE J. Sel. Areas Commun.* **31**, 1728–1740. (doi:10.1109/JSAC.2013.130907)
19. Hu J, Yan S, Shu F, Wang J, Li J, Zhang Y. 2017 Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays. *IEEE Access* **5**, 1658–1667. (doi:10.1109/ACCESS.2017.2653182)
20. Ren K, Su H, Wang Q. 2011 Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wirel. Commun.* **18**, 6–12. (doi:10.1109/MWC.2011.5999759)
21. Wang Q, Su H, Ren K, Kim K. 2011 Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In *Proc. 2011 IEEE INFOCOM, Shanghai, China, 10–15 April 2011*, pp. 1422–1430.
22. Yang N, Yeoh PL, Elkashlan M, Schober R, Collings IB. 2013 Transmit antenna selection for security enhancement in MIMO wiretap channels. *IEEE Trans. Commun.* **61**, 144–154. (doi:10.1109/TCOMM.2012.12.110670)
23. Zou Y, Zhu J, Wang X, Leung VCM. 2015 Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network* **29**, 42–48. (doi:10.1109/MNET.2015.7018202)
24. Rahaim M, Abdalla I, Ayyash M, Elgala H, Khreishah A, Little TDC. 2019 Welcome to the CROWD: design decisions for coexisting radio and optical wireless deployments. *IEEE Network* **33**, 174–182. (doi:10.1109/MNET.2019.1800297)
25. Elgala H, Mesleh R, Haas H. 2011 Indoor optical wireless communication: potential and state-of-the-art. *IEEE Commun. Mag.* **49**, 56–62. (doi:10.1109/MCOM.2011.6011734)

26. Lv X, Mu Y, Li H. 2013 Key distribution for heterogeneous public-key cryptosystems. *J. Commun. Netw.* **15**, 464–468. (doi:10.1109/JCN.2013.000085)
27. Zhu L, Zhan Z. 2015 A random key management scheme for heterogeneous wireless sensor network. In *Proc. 2015 Int. Conf. on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 5–7 August 2015*, pp. 1–5.
28. Wang S, Li W, Lei J. 2018 Physical-layer encryption in massive MIMO systems with spatial modulation. *China Commun.* **15**, 159–171. (doi:10.1109/CC.2018.8485478)
29. Di Renzo M, Haas H, Ghrayeb A, Sugiura S, Hanzo L. 2014 Spatial modulation for generalized MIMO: challenges, opportunities, and implementation. *Proc. IEEE* **102**, 56–103. (doi:10.1109/JPROC.2013.2287851)
30. Wu F, Yang L, Wang W, Kong Z. 2015 Secret precoding-aided spatial modulation. *IEEE Commun. Lett.* **19**, 1544–1547. (doi:10.1109/LCOMM.2015.2453313)
31. Yang L. 2011 Transmitter preprocessing aided spatial modulation for multiple-input multiple-output systems. In *Proc. 2011 IEEE 73rd Vehicular Technology Conf. (VTC Spring), Budapest, Hungary, 15–18 May 2012*, pp. 1–5.
32. Guan X, Cai Y, Yang W. 2012 On the secrecy mutual information of spatial modulation with finite alphabet. In *Proc. 2012 Int. Conf. on Wireless Communications and Signal Processing (WCSP), Huangshan, China, 25–27 October 2012*, pp. 1–4.
33. Wu F, Zhang R, Yang L, Wang W. 2016 Transmitter precoding-aided spatial modulation for secrecy communications. *IEEE Trans. Veh. Technol.* **65**, 467–471. (doi:10.1109/TVT.2015.2395457)
34. Cumanan K, Xing H, Xu P, Zheng G, Dai X, Nallanathan A, Ding Z, Karagiannidis GK. 2017 Physical layer security jamming: theoretical limits and practical designs in wireless networks. *IEEE Access* **5**, 3603–3611. (doi:10.1109/ACCESS.2016.2636239)
35. Chen Y, Wang L, Zhao Z, Ma M, Jiao B. 2016 Secure multiuser MIMO downlink transmission via precoding-aided spatial modulation. *IEEE Commun. Lett.* **20**, 1116–1119. (doi:10.1109/LCOMM.2016.2549014)
36. Yang P, Qiu X, Mu F. 2020 Artificial noise-aided secure generalized spatial modulation for multiuser transmission. *IEEE Commun. Lett.* **24**, 2416–2420. (doi:10.1109/LCOMM.2020.3011284)
37. Wang L, Bashar S, Wei Y, Li R. 2015 Secrecy enhancement analysis against unknown eavesdropping in spatial modulation. *IEEE Commun. Lett.* **19**, 1351–1354. (doi:10.1109/LCOMM.2015.2440353)
38. Wang X, Wang X, Sun L. 2016 Spatial modulation aided physical layer security enhancement for fading wiretap channels. In *Proc. 2016 8th Int. Conf. on Wireless Communications Signal Processing (WCSP), Yangzhou, Jiangsu, China, 13–15 October 2016*, pp. 1–5.
39. Huang Y, Wen M, Zheng B, Cheng X, Yang L, Ji F. 2019 Secure precoding aided spatial modulation via transmit antenna selection. *IEEE Trans. Veh. Technol.* **68**, 8893–8905. (doi:10.1109/TVT.2019.2930071)
40. Mesleh RY, Haas H, Sinanovic S, Ahn CW, Yun S. 2008 Spatial modulation. *IEEE Trans. Veh. Technol.* **57**, 2228–2241. (doi:10.1109/TVT.2007.912136)
41. Mesleh R, Elgala H, Haas H. 2011 Optical spatial modulation. *IEEE/OSA J. Opt. Commun. Networking* **3**, 234–244. (doi:10.1364/JOCN.3.000234)
42. Pan G, Ye J, Ding Z. 2017 Secure hybrid VLC-RF systems with light energy harvesting. *IEEE Trans. Commun.* **65**, 4348–4359. (doi:10.1109/TCOMM.2017.2709314)
43. Pan G, Ye J, Ding Z. 2017 Secrecy outage analysis of hybrid VLC-RF systems with light energy harvesting. In *Proc. 2017 IEEE 18th Int. Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Sapporo, Japan, 3–6 July 2017*, pp. 1–5.
44. Marzban MF, Kashef M, Abdallah M, Khairy M. 2017 Beamforming and power allocation for physical-layer security in hybrid RF/VLC wireless networks. In *Proc. 2017 13th Int. Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017*, pp. 258–263.
45. Kumar A, Garg P, Gupta A. 2020 PLS analysis in an indoor heterogeneous VLC/RF network based on known and unknown CSI. *IEEE Syst. J.* **15**, 1–9.
46. Hussein AF, Elgala H. 2020 Wireless link pairing toward secured 6G networks. *Opt. Lett.* **45**, 4005–4008. (doi:10.1364/OL.395542)
47. Khadr MH, Elgala H, Ayyash M, Little T, Khreishah A, Rahaim M. 2018 Security aware spatial modulation (SA-SM). In *Proc. 2018 IEEE 39th Sarnoff Symp., Newark, NJ, 24–25 September 2018*, pp. 1–6.

48. Zhu R, Shu T, Fu H. 2017 Empirical statistical inference attack against PHY-layer key extraction in real environments. In *Proc. MILCOM 2017 - 2017 IEEE Military Communications Conf. (MILCOM), Baltimore, MD, 23–25 October 2017*, pp. 46–51.
49. Haas H, Yin L, Wang Y, Chen C. 2016 What is LiFi? *J. Lightwave Technol.* **34**, 1533–1544. (doi:10.1109/JLT.2015.2510021)
50. Duvnjak F, Ožegović J, Kristić A. 2015 Heterogeneous Wi-Fi and VLC (RF-optical) wireless access architecture. In *Proc. 2015 23rd Int. Conf. on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 16–18 September 2015*, pp. 310–314.
51. Elgala H, Mesleh R, Haas H. 2009 Indoor broadcasting via white LEDs and OFDM. *IEEE Trans. Consum. Electron.* **55**, 1127–1134. (doi:10.1109/TCE.2009.5277966)
52. Qian X, Deng H, He H. 2018 Joint synchronization and channel estimation of ACO-OFDM systems with simplified transceiver. *IEEE Photonics Technol. Lett.* **30**, 383–386. (doi:10.1109/LPT.2018.2792402)
53. Fath T, Haas H. 2013 Performance comparison of MIMO techniques for optical wireless communications in indoor environments. *IEEE Trans. Commun.* **61**, 733–742. (doi:10.1109/TCOMM.2012.120512.110578)
54. Wang Y, Haas H. 2015 Dynamic load balancing with handover in hybrid Li-Fi and Wi-Fi networks. *J. Lightwave Technol.* **33**, 4671–4682. (doi:10.1109/JLT.2015.2480969)
55. Classen J, Chen J, Steinmetzer D, Hollick M, Knightly E. 2015 The spy next door: eavesdropping on high throughput visible light communications. In *Proc. of the 2nd Int. Workshop on Visible Light Communications Systems VLCS '15, Paris, France, 7–11 September 2015*, pp. 9–14. New York, NY: ACM.
56. Minn H, Bhargava VK, Letaief KB. 2003 A robust timing and frequency synchronization for OFDM systems. *IEEE Trans. Wirel. Commun.* **2**, 822–839. (doi:10.1109/TWC.2003.814346)
57. Liu Y, Yu H, Ji F, Chen F, Pan W. 2014 Robust timing estimation method for OFDM systems with reduced complexity. *IEEE Commun. Lett.* **18**, 1959–1962. (doi:10.1109/LCOMM.2014.2358234)
58. Kumar A, Garg P. 2018 Physical layer security for dual-hop FSO/RF system using generalized $\Gamma\Gamma/\eta - \mu$ fading channels. *Int. J. Commun. Syst* **31**, 1–12.
59. Fotohabady V, Said F. 2011 Comparison of the Rayleigh and Nakagami fading channels MIMO multicarrier system. In *Proc. 2011 Wireless Advanced, London, UK, 20–22 June 2011*, pp. 295–300.
60. Kashef M, Ismail M, Abdallah M, Qaraqe KA, Serpedin E. 2016 Energy efficient resource allocation for mixed RF/VLC heterogeneous wireless networks. *IEEE J. Sel. Areas Commun.* **34**, 883–893. (doi:10.1109/JSAC.2016.2544618)
61. Ganesan S, Mesleh R, Ho H, Ahn CW, Yun S. 2006 On the performance of spatial modulation OFDM. In *Proc. 2006 40th Asilomar Conf. on Signals, Systems and Computers, Pacific Grove, CA, 29 October–1 November 2006*, pp. 1825–1829.
62. Zhou B, Xiao Y, Yang P, Li S. 2011 An iterative CFO compensation algorithm for distributed spatial modulation OFDM systems. In *Proc. 2011 7th Int. Conf. on Wireless Communications, Networking and Mobile Computing, Wuhan, China, 23–25 September 2011*, pp. 1–4.
63. Rajashekar R, Hari KVS, Hanzo L. 2014 Reduced-complexity ML detection and capacity-optimized training for spatial modulation systems. *IEEE Trans. Commun.* **62**, 112–125. (doi:10.1109/TCOMM.2013.120213.120850)
64. Huang G, Zhou H, Ding X, Zhang R. 2012 Extreme learning machine for regression and multiclass classification. *IEEE Trans. Syst. Man Cybern. B Cybern.* **42**, 513–529. (doi:10.1109/TSMCB.2011.2168604)
65. Chang CC, Lin CJ. 2011 LIBSVM: a library for support vector machines. *ACM Trans. Intell. Syst. Technol.* **2**, 1–27. (doi:10.1145/1961189.1961199)