Machine Learning for Physical Layer Security: Limitations, Challenges and Recommendation

Reem Melki[1], Hassan N. Noura[2], Ali Chehab[1], and Raphael Couturier[2]

[1] Electrical and Computer Engineering, American University of Beirut (AUB), Beirut, Lebanon
[2]Univ. Franche-Comté (UFC), FEMTO-ST Institute, CNRS, Belfort, France

Abstract—**The properties and features of wireless channels have recently attracted the attention of researchers since they include valuable and powerful parameters for security services. This has paved the way for a new security paradigm, Physical Layer Security (PLS). To further improve the performance and security of such technology, it is recently being combined with machine learning algorithms to provide authentication, confidentiality and intrusion detection. Motivated by the novel advancements in this field, we present a brief overview of the different machine learning techniques and algorithms that offer PLS-based security services. These techniques are discussed in details to shed the light on the existing methods in the literature. We also propose several recommendations for enhancing the performance and efficiency of the presented schemes.**

Keywords— Machine learning; physical layer security; authentication, confidentiality, intrusion detection system.

I. Introduction

Machine Learning (ML) is a fundamental branch of artificial intelligence that allows a system to parse data, learn from it and predict future outcomes. This is mainly done without the intervention of human assistance. In particular, machine learning algorithms form a mathematical model based on a specific amount of ”training data”, which can be either labeled or unlabeled, to enable correct decision making and precise predictions regarding future input data. Lately, this technology gained a lot of attention due to its applicability within numerous applications such as image classification, self-driving cars, natural language processing, speech recognition, smart healthcare, and search engine result refining [1]. Additionally, machine learning has played an important role in enhancing and ensuring robust security in terms of user/device authentication, data protection and confidentiality and most importantly behavior-based intrusion detection. Some examples of ML-based security include email spam detection, malware filtering and online fraud detection.

Typically, security solutions are based on cryptographic and non-cryptographic approaches (Figure 1). The cryptographic ones can be divided into algorithms and protocols. On the other hand, non-cryptographic approaches use different solutions such as physical protection and ML, which are the main focus of this paper. Traditional cryptographic algorithms rely on the Shannon's concept, which requires the iteration of a round function multiple times. However, this type of solutions exhibits high computational complexity and relatively large delays, which necessitates the introduction of more efficient techniques [2], [3], [4]. With the help of machine learning algorithms, security systems can mitigate future attacks and adapt to changing behavior in real-time, which is crucial since some malware and attacks are frequently modified to evade the security measures. This offers protection for legitimate users and their data when they communicate with each other, and it safeguards data that is stored in the cloud.

In this paper, we focus on machine learning techniques that are adopted for physical layer security (PLS), a new security paradigm that exploits the inherent randomness and dynamicity of the physical layer to secure data in transit over wireless channels. The unique features and properties of wireless channels are extracted and used for securing data. Several works in the literature have resorted to machine learning algorithms to greatly enhance systems' security due to their ability to analyze threats, learn patterns and prevent malware and attacks. Moreover, such techniques enable a system to automatically respond to changing behavior and to adapt to new types of risks and threats. Based on the underlying security service, the presented schemes are divided into three groups: authentication, confidentiality, and intrusion detection. An overview of these schemes is presented and each scheme is described in details. We also highlight the limitations of each method and we propose ways to overcome these drawbacks.

The rest of the paper is organized as follows. Section II presents some background information on machine learning and related algorithms. Section III presents an overview of the schemes presented in the literature, and a thorough discussion of each of the schemes. Section IV presents the current challenges in this field, and Section V discusses the lessons learnt. Section VI presents some recommendations to enhance the existing schemes. Finally, Section VII concludes the paper and presents future prospects.

II. Background

Machine learning is mainly divided into two types: supervised and unsupervised [5], [6].

For the former learning method, the machine is first trained using labeled data, based on which, the machine develops a function that predicts the right answer/category of future input data. Supervised learning is divided into two sub-types, regression and classification. Regression is used when the input is continuous (for example, ”height”). In contrast, classification is used for simple data such as binary (”yes” or ”no”) or multi-classification, in the case of multiple categories) [7], [8]. Some examples of supervised machine learning algorithms include decision trees, linear regression, K-NN (k nearest neighbors), support vector machine and Naive Bayes. Supervised learning has many advantages some of which are:

- It is specific and accurate since the machine is trained to distinguish the different classes and features of the input data.
- One is able to determine the number of required classes.
- Input data is well known and labeled.
- It is a simple process.
- Once training is complete, the training data can be discarded from memory.

On the other hand, this technique suffers from some disadvantages:

- The input data should be divided and labeled correctly, otherwise the model will not function properly.
- The process is not done in real time; the input data should be trained offline prior to the prediction process.
- In some cases, the required training data is not available.
- The training process is time consuming.

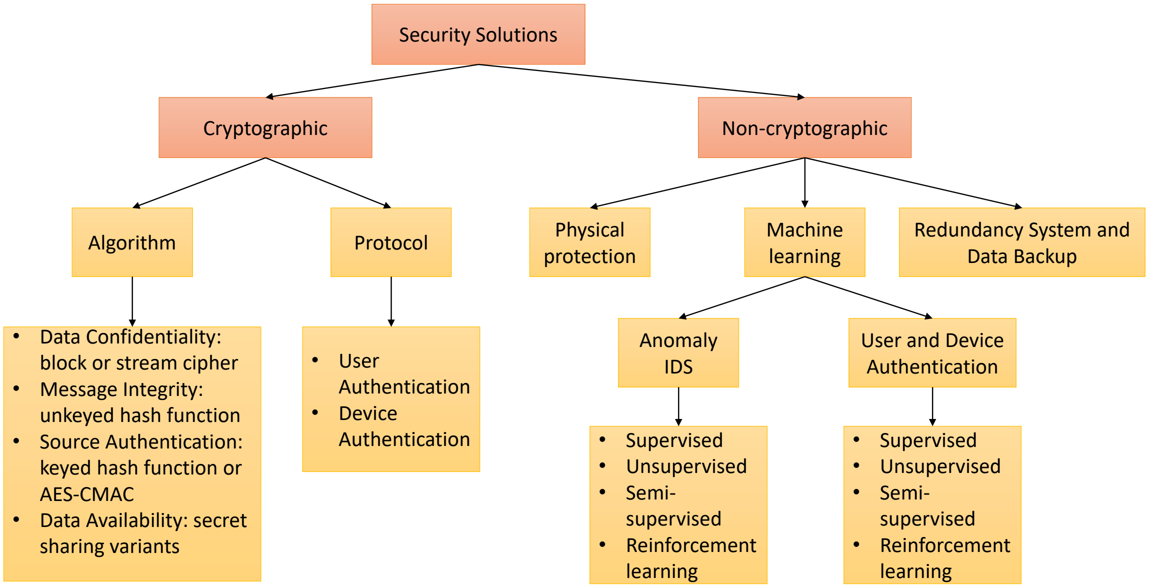

Fig. 1: Classification of security techniques

- It is limited because when the data does not belong to any of the labeled classes, the output will be erroneously attributed to one of the existing classes.
- Supervised learning does not provide new information from the training data.

Typically, supervised learning is used in file analysis such as antivirus use cases where the applications and files are already known and documented.

In contrast, unsupervised machine learning is used for network traffic analysis, whereby data is frequently changing (dynamic) [9]. As such, the labeling is scarce since the behavior is constantly changing and anomalies are continuously adapting. Therefore, unsupervised learning does not require human guidance, training data or labeled classes, to predict future data. Specifically, this technique groups unknown data based on their similarities and differences. The main task here is to be able to distinguish the different features, the structure and the hidden patterns of the input data.

Unsupervised learning algorithms fall under two categories: clustering and association. For the former, the data is grouped based on similarities, whereas for the latter, the data is grouped based on the relation between their attributes. Some unsupervised machine learning algorithms include K-means clustering, dimensionality reduction, neural networks and deep learning. These algorithms have multiple advantages:

- Data is analyzed in real time.
- Unlabeled data is easier to obtain.
- There is no need to label the data and specify the different classes. The algorithm figures out this task on its own.
- They are Less computationally complex than supervised learning; offline analysis is not needed.
- The machine is able to learn new features and adapt to changing data.

The disadvantage of unsupervised learning is that it is less accurate and less specific since data is not labeled and there are no pre-defined classes.

Machine learning techniques can also be semi-supervised, where two types of data are used in the training process: labeled data and unlabeled data [10]. In this class, the number of labeled data is far less than that of the unlabeled data, and thus, overcoming some of the disadvantages of supervised learning such as the scarcity of labeled data. Finally, reinforcement learning, which is the fourth paradigm within machine learning, enables the model to make decisions in complex environments [11]. The classification of machine learning types and algorithms is illustrated in Fig. 2.

Recently, machine learning has been adopted to enhance existing physical layer security schemes and to increase their robustness against various attacks. Specifically, machine learning has been used to analyze the physical layer properties of shared wireless channels, such as the channel state information and carrier frequency offset, to realize different security services such as authentication, confidentiality and intrusion detection. As such, legitimate users are able to detect any abnormal behavior caused by adversaries.

In the following section, we will present and describe the schemes in the literature that combine the notion of machine learning and physical layer security.

III. Machine Learning for Physical Layer Security

Machine learning can be used to achieve authentication, confidentiality and intrusion detection. The schemes in the literature will be divided according to the previous categories and they will be detailed next.

A. User and Device Authentication based on Machine Learning

The importance of machine learning in achieving authentication is highlighted in [12]. In particular, the authors classify machine learning algorithms into two groups: parametric/non-parametric (depending on whether there are specific forms of training functions) and supervised/unsupervised/reinforcement learning (depending on whether there are labeled samples in the database). The authors

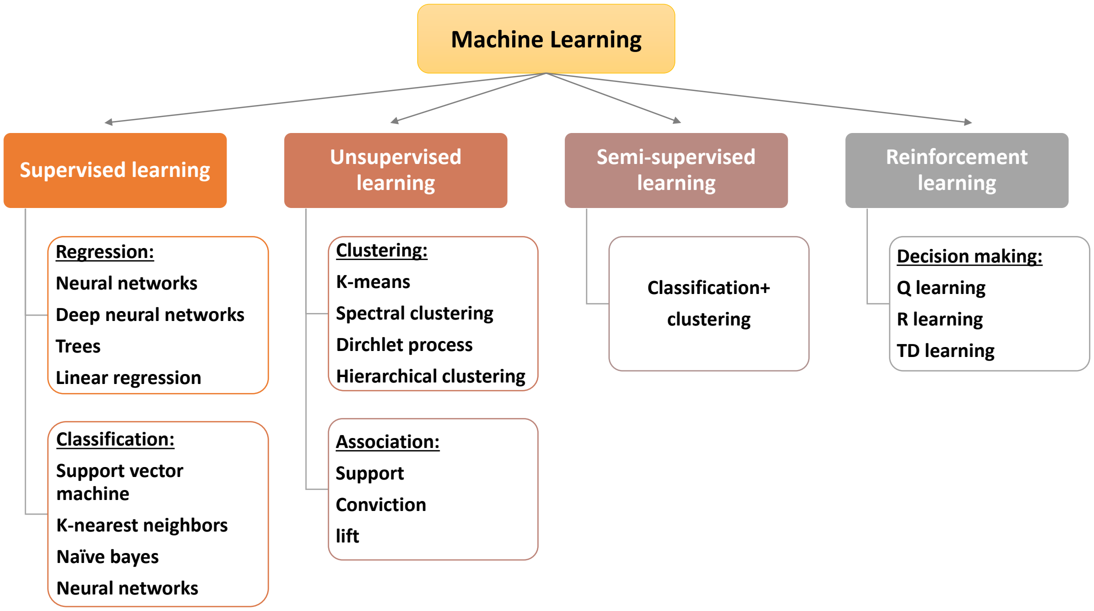

Fig. 2: Classification of machine learning techniques

also conducted several tests to evaluate the performance of intelligent schemes and static schemes in terms of miss-detection rate and computational costs. The obtained results showed that machine learning has a lower miss-detection rate than static approaches, especially those depending on multiple features, and it requires lower computational costs.

1) Authentication based on Physical Channel Features: The physical channel properties are used as key features to train input data to achieve device authentication. Examples of channel properties are channel state information, time of arrival and carrier frequency offset. In [13], the authors combined physical layer security and machine learning to authenticate communicating users at the physical layer. Upon the reception of packets, both users perform authentication by extracting the channel state information of each packet from the received pilots. Typically, the difference between the channel state information matrices should be below a specific threshold for the authentication to be successful. In particular, the ϵ-greedy strategy is applied to identify the optimal threshold that maximizes the gain, which is expressed in terms of the probabilities of the four possible cases: true positive, true negative, false positive and false negative.

Similarly, the authors in [14] presented a physical layer authentication mechanism based on machine learning to authenticate users in Multiple-Input Multiple-Output (MIMO) systems. The proposed scheme exploits the randomness of the channel response and the location of users to perform classification with minimum error. Specifically, three steps are considered: feature extraction, feature selection and classification. The Channel Impulse Response (CIR) features are divided into four groups: 1) antenna processing (minimum, maximum, average and concatenation), 2) signal transform (original, Discrete Cosine Transform (DCT), Fast Four Transform (FFT), and gradient), 3) information enhancement (original, auto-correlation) and 4) complex signal processing (no process, real, imaginary, gain, phase, arc). The high dimensions of obtained features are reduced using the Neighborhood Component Analysis (NCA) algorithm. Moreover, the chosen features are classified using a Radial Basis Function (RBF) kernel-based Support Vector Machine (SVM).

Channel matrices are also used in [15] as features to achieve physical layer authentication based on Machine Learning. Unlike the traditional threshold-based physical layer authentication schemes (stationary scenarios), the presented solution benefits from adaptive classification based on machine learning, which suits mobile scenarios. For the offline training phase, four ML classification algorithms are considered, the Decision Tree (DT), the Support Vector Machine (SVM), the K-Nearest Neighbors (KNN), and the ensemble learning. The same methodology was applied in [16].

In [17], the authors relied on deep learning to extract blind features form physical channels to authenticate users. In [18], the authors presented an authentication mechanism that consists of three main phases. First, the channel state information is extracted, after estimating the channel. Then, the dimension of the channel matrix is reduced using Karhunen-Loeve Transform (KLT) to decrease the computational complexity. Finally, a Gaussian Mixture Model-based (GMM) authentication algorithm is performed. The parameters of the GMM function can be estimated using the Expectation Maximization (EM) algorithm whose parameters can be initialized by the Linde-Buzo-Gray (LBG) algorithm. This algorithm trains the channel data, and then, the mean and variance are utilized in the Gaussian Mixture Model.

By leveraging the physical channel characteristics and machine learning techniques, the authors in [19] presented two authentication schemes based on different algorithms, the support vector machine-based authentication algorithm, and the linear Fisher Discriminant Analysis-based scheme. Both of these schemes rely on three main features, the received signal strength, the time of arrival and the correlation of cyclic feature vectors.

2) Authentication based on the "You Are" Factor: Another approach to ensure robust authentication is by using the unique features of the user that cannot be changed such as fingerprint, physical unclonable functions (PUF), and facial features.

In [20], the authors leveraged the uniqueness of Physical Unclonable Functions in transmitters to achieve on-the-fly authentication. Specifically, Artificial Neural Networks (ANN) are used to train data according to the following features: local oscillator frequency offset, channel information, DC offset and I-Q mismatch in transmitters. Since these features vary greatly from one device to the other (Radio Frequency properties) as a result of fabrication, they can be used to achieve proper authentication.

In [21], the security of automobiles was achieved through driver fingerprinting. The authors conducted a comprehensive study on behavioral characteristics of drivers in two types of vehicles, Luxgen U5 SUV and Buick Regal. This is of great significance since, currently, the identity of drivers is not monitored in real-time. The main goal of the proposed scheme is to ensure the safety of people's properties and even lives using an efficient and robust real-time automobile driver fingerprinting scheme.

Differently, the authors in [22] relied on the Radio frequency (RF) fingerprint recognition technology in the authentication process. In this work, the radio frequency characteristics are used to authenticate users/devices since these properties are unique and cannot be imitated. The proposed scheme is based on dimensional reduction and machine learning. The same concept was adopted in [23], where RF fingerprint features are extracted. The behavioral characteristics of smartphones were used in [24], along with machine learning, to authenticate smartphones. Similarly, the authors in [25] approximated the behavior of a device using features extracted from the device network traffic.

In contrast, the authors in [26] leveraged the signal features to authenticate devices. They used the wavelet transform to decompose signals and extract feature matrices of the samples.

3) Authentication based on the ”You Do” Factor: This factor is based on the actions performed by the device. One main example is the traffic generated by users. It can be listed under the ”you are” factor and the ”you do”, since network traffic is unique for each user and it is a result of a set of actions done by the user at the same time.

In [27], the authors classified the devices' types based on their unique fingerprints, which are attributed to the number of packets generated during the setup phase. The authors performed classification in two phases: during the first phase, trained classifiers are used to classify device fingerprints. Afterwards, the most suitable (probable) device class is identified. This step is crucial when a device is classified as belonging to several classes. Differently, self-learning was adopted in [28], where the device model is specified based on its signature. A similar concept was adopted in [29], where the authors used the patterns of physical layer communication to recognize a device connected to a certain network.

On the other hand, traffic features were utilized in [30] to identify Internet-of-Things (IoT) devices. Some of these traffic features include the packet size and inter-arrival time. Similarly, a multi-stage classifier was used in [31]. First, classification is done taking into consideration port numbers, domain names, and cipher suites. Next, another classifier uses statistical features such as the flow volume, flow rate, flow duration, sleep time, DNS interval, and NTP interval. The authors in [32] and in [33] also classified devices based on network traffic flows.

In [34], physical layer fingerprinting was considered for device classification. Some of the features that are adopted are signal power, attenuation, and interference. Differently, signal imperfections were used to create user profiles in [35], [36], by monitoring and differentiating different types of devices present in a smart home.

The features and characteristics of IoT devices were defined based on the packet contents in [37]. In their recent work, the authors in [38] utilized basic flow features such as size, timestamp, and direction to recognize the type of IoT devices and to detect traffic attacks.

The discussed schemes are summarized in Table I.

B. Intrusion Detection Systems using Machine Learning

In [39] an attack detection scheme was presented. It consists of feature generation and detection modelling. The feature generation mechanism depends on one variable (univariate) or on multiple variables (multivariate). In the former case, the features depend on statistical measurements such as the minimum, the maximum and the standard deviation. For the later case, three groups of features are calculated using multiple variables. The first group evaluates the relation (difference) between a pair of measurements (defined by domain experts or learned from the data). The second group is physics-based and uses the difference between the measurements and the model's predictions. The last group is learning-based, and it is completely data driven. It learns from multiple measurements using deep learning. As the number of stacked shallow learning blocks increases, the learned data become more informative, more robust to variations, and will have more abstract aspects. For this phase, the authors utilized the stacked de-noising auto-encoder (SDAE) as the deep learning architecture. For detection modelling, the Extreme Learning Machine (ELM) was employed.

The authors in [40] proposed a directional reactive jamming scheme based on machine learning. In particular, the transmitter sends a broadcast signal to the eavesdropper and the legitimate receiver, which in return replies with preamble sequences. Consequently, the transmitter extracts the real and imaginary components (features) of the Channel State Information (CSI), and divide them into two clusters based on the K-means algorithm. Afterwards, a support vector machine (SVM) with soft threshold is trained with the labeled data. Using this technique, the transmitter directs its beam to send interference signals to the eavesdropper to degrade its channel. One drawback of this scheme is the assumption that the transmitter is able to obtain the CSI of the eavesdropper, which might not be possible in most cases.

On the other hand, the authors in [41] proposed a fault detection mechanism based on neural networks for cooperative adaptive cruise control systems to prevent collisions among vehicles. The proposed technique utilizes a fuzzy decision-making system, which maintains a safe gap between the vehicles. The inputs are the follower vehicle's speed and speed error (based on the difference of the actual and the estimated speed of the leading vehicle), whereas the output is the additional safe distance added to the present gap to prevent possible incidents.

Also, the authors in [42] benefited from machine learning and the multiple features of electromagnetic signals to identify abnormal electromagnetic signals at the physical layer.

An intrusion detection and location system based on machine learning was proposed in [43]. The tasks of the proposed solution were divided into three categories: detection, branch location, and position determination. The first two tasks are formulated as supervised classification based the channel impulse response and the position determination task as supervised regression tasks. The support vector machine (SVM) and boosting ML algorithms were considered for both, classification and regression.

Since temporal information (information in previous states) can be useful to detect attacks in vehicular systems, the authors

TABLE I: The summary of machine learning schemes that achieve device authentication

Reference	Features	Machine learning algorithm	Type
[13]	Channel state information from pilot packets	ϵ-greedy strategy to identify the optimal threshold	Supervised
[14]	Channel Impulse Response (CIR) features: 1) antenna processing, 2) signal transform, 3) information enhancement and 4) complex signal processing	Basis Function (RBF) kernel-based Support Vector Machine (SVM)	Supervised
[15]	Channel state information	Decision Tree (DT), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and ensemble learning	Supervised
[17]	Blind features	Deep learning models	Unsupervised
[18]	Channel state information	Gaussian Mixture Model-based (GMM) authentication algorithm	Unsupervised
[19]	The received signal strength, the time of arrival and the correlation of cyclic feature vectors	Support vector machine-based authentication algorithm and the linear fisher discriminant analysis-based authentication scheme	Supervised
[20]	Local oscillator frequency offset, channel information, DC offset and I-Q mismatch in transmitters	Artificial Neural Networks (ANN)	Supervised

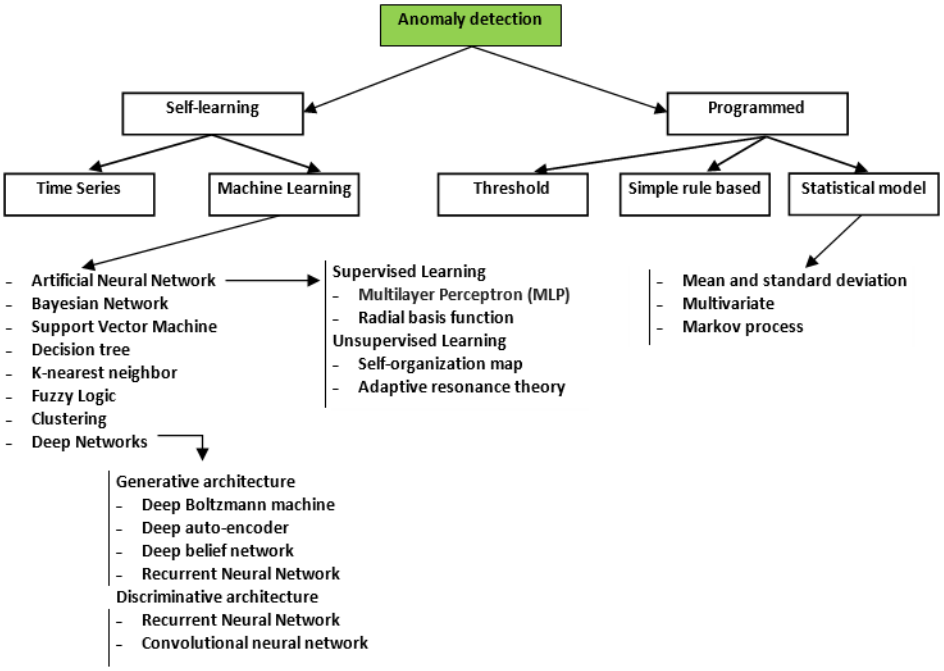

Fig. 3: Classification of anomaly detection techniques

of [44] used recurrent neural networks instead of feed-forward neural networks, which look for occurrences of the same patterns in the feature-space based on current state. In recurrent neural networks, the occurrence of attacks depends on input features in the previous as well as current states (state refer to period of time). The features that were considered are the cyber input features (related to communication and processing) and the physical input features (related to the physical properties). The first type includes network incoming and outgoing traffic rates, CPU utilization and the data being written on the disk. The second type includes encoder (measuring the difference between two consecutive encoder value readings in a fixed period of time), accelerometer (the vibration of the chassis), power (the overall power consumption by the vehicle) and current (the overall current drawn by the vehicle).

In [45], the authors conducted several experiments to study the importance of machine learning in detecting physical layer attacks in optical networks. They also listed the types of supervised ML algorithms used in the classification process, artificial neural networks, support vector machine, Gaussian process, decision tree, random forests, naive bayes, nearest neighbors, quadratic discriminant analysis. Similarly, the authors in [46] studied the effect of machine learning in detecting attacks in software defined networks.

In [47], the authors proposed the detection of primary user emulation attack in cognitive radio networks based on machine learning. Here, four main features were considered: the mean of the channel impulse response values, the variance (value fluctuations corresponding to the mean), skewness (asymmetry of value with respect to the mean) and the difference between the maximum and minimum values. For the training and testing steps, six classification models were considered: Logistic Regression (LR), Linear Discriminant Analysis (LDA), k-Nearest Neighbors (KNN), Decision Tree Classifier (DTC), Gaussian Naive Bayes (NB), and Support Vector Machine (SVM).

The authors of [48], proposed a machine learning-based technique (un-supervised) to detect malicious relays in cooperative networks. They utilized Support Vector Machines (SVM) functions, k-Nearest Neighbors (k-NN), and Isolation Forest. Moreover, three main features were considered: amplitude of the symbol, the position of the symbol in the constellation and the phase difference between two consecutive symbols.

In [49], a multi-stage scheme was proposed to detect four jamming attacks in Cloud Radio Access Networks. Specifically, the proposed machine learning-based intrusion detection system identifies five scenarios: normal traffic (no attack), constant jammer (jammer sending random data constantly), random jammer (the jammer remains idle during the sleeping period and acts as a constant jammer during the jamming period), deceptive jammer (the jammer sends illegitimate packets and not random data) and the reactive jammer (jammer sends illegitimate packets only when data transmission is detected on a specific channel). The authors processed and classified the data using the Multilayer Perceptron (MLP). If the traffic is classified as normal, the Kernelized Support Vector Machine is utilized to reduce the false negative rate. For feature extraction, the principal component analysis technique was used to identify the most significant features in wireless sensor networks, which is a statistical technique used mainly to decrease dimensionality. As such, the authors identified the most important ten features.

Table II summarises the machine learning-based schemes that achieve intrusion detection. Figure 3 also presents a taxonomy of the anomaly detection schemes based on machine learning techniques.

C. Confidentiality using Machine Learning

In [50], the authors used machine learning to provide proper beamforming and power allocation. In particular, the channel state information of the eavesdropper and the legitimate receiver are evaluated so that only the legitimate receiver is able to correctly recover the original data. However, obtaining the channel state information of a passive eavesdropper is not always possible, and hence, the scheme should not depend on the adversary's channel.

In [51], the authors presented the transmit antenna selection (TAS) as a transmission strategy based on machine learning. The scheme accounts for the case of full CSI (CSI of eavesdropper is known) as well as partial CSI (CSI of eavesdropper is unknown). First, the obtained CSI values are transformed into real values and then normalized. Next, SVM and the naive-Bayes are used to select the optimal antenna that maximizes the channel secrecy.

To enhance the security of Smart Grids, the authors in [52] presented a brief survey of the threats and vulnerabilities of smart grids, and possible countermeasures based on machine learning. The same approach was also considered for securing cyber-physical systems in [53].

Differently, the authors in [54] used supervised machine learning (neural networks) to choose the optimal relay among a set of relays, based on the maximum achievable secrecy rate. The authors assumed that the information related to the adversary's channel is available, which again may not be possible in most cases.

In [55], the authors proposed a low probability of intercept communication scheme based on machine learning. They used the Plane Spiral Orbital Angular Momentum (OAM) in the radio domain to secure transmitted data between the communicating entities. The transmitter modulates data using several PS-QAM modes and relies on supervised SVM to evaluate the performance of communication and to restore symbols from high dimensional space. The receiver, on the other hand, demodulates the received data and uses the K-means technique (unsupervised) to intercept the data, measure its similarity and to cluster it, accordingly.

In [56], the authors presented a brief overview of cyber-physical systems, their associated security threats at different layers and possible ways to mitigate them. To enhance the security of cyber-physical systems, they proposed the use of machine learning. However, the proposal suffers from multiple security vulnerabilities mainly data poisoning during training and ML architectural intrusions.

In [57], the authors illustrated the benefits of machine learning at the different layers. They indicated that deep learning plays an important role at the physical layer of wireless networks since it can be used for interference alignment, anti-jamming schemes, modulation classification and types, and physical coding.

IV. Machine Learning Security Challenges and Open Issues

Although machine learning has been used to enhance many aspects of network security, there are some remaining challenges associated with this technology. One main issue is compromising the privacy and identity of devices such as IoT (Internet-of-Things) devices. By applying machine learning to the traffic, one can identify the different communicating devices. Another important point is the heterogeneous types of the data having different characteristics and properties, which is accounted for in machine learning algorithms. Also, with the large number of already existing algorithms, it is hard to choose the appropriate algorithm for a specific problem. Therefore, more research should be directed towards specifying the characteristics, advantages and disadvantages of each of the algorithms [58], [59].

Moreover, it has been shown that machine learning requires a significant overhead in terms of computational complexity, which can be a challenge for current and emerging restricted devices. There is a need for efficient schemes that strike the appropriate balance between the security level and performance [58], [59].

When addressing security issues in a system, it is important to have a robust key generation and distribution scheme. Currently, there are no such schemes available when using machine learning for physical layer security. Also, there is a need to enhance the detection of behavior-based attacks, and more efforts should be exerted to efficiently defend against DDoS (Distributed Denial of Service) attacks [58], [59].

There is still a lot of work to be done in this area, which paves the way for researchers to explore this topic and the numerous opportunities for contribution [58], [59].

V. Lessons Learnt

Two important takeaways that need to be emphasized when dealing with machine learning are the choice of the algorithm(s) and the associated complexity. Currently, there are many machine learning algorithms within the supervised and unsupervised domains. More research should be dedicated towards assessing the capabilities of each of the algorithms and their suitability for the different existing problems. This would help researchers in the selection process of the best fitted algorithm for the problems they are tackling. Also, there is the need for more efficient (low computational complexity) machine learning algorithms while maintaining the same performance.

VI. Recommendation

Most security schemes in the literature rely on a single factor to secure data, such as the case in authentication and confidentiality processes. In order to enhance the security level of existing PLS schemes that are based on machine learning, one needs to resort to two factors instead of just one. For example, users can use channel information, such as the channel state information, along with the unique features of the communicating devices, such as physical unclonable functions, to authenticate each others. Also, users can use reinforcement learning, which allows devices to make decisions

TABLE II: The summary of machine learning schemes that achieve anomaly intrusion detection against jamming attacks

Reference	**Features**	**Machine learning algorithm**	**Type**
[39]	Uni-variate, statistical measurements: minimum, the maximum and the standard deviation, or multi-variate	stacked de-noising auto-encoder (SDAE) as the deep learning architecture and Extreme Learning Machine (ELM)	Supervised
[40]	Channel State Information (CSI)	Support Vector Machine (SVM)	Supervised
[41]	-	Neural networks	Unsupervised
[42]	-	Apriori algorithm	Unsupervised
[43]	Channel impulse response	Support Vector Machine (SVM)	Supervised
[44]	The cyber input features and the physical input features	Neural networks	Supervised
[47]	The mean of the channel impulse response values, the variance, skewness and the difference between the maximum and minimum values	Logistic Regression (LR), Linear Discriminant Analysis (LDA), k-Nearest Neighbors (KNN), Decision Tree Classifier (DTC), Gaussian Naive Bayes (NB), and Support Vector Machine (SVM)	Supervised
[48]	-	Support Vector Machines (SVM) functions, k-Nearest Neighbors (k-NN), and Isolation Forest	Unsupervised
[49]	Ten features are identified	Multi-layers Perceptron (MLP)	Supervised

and to take action in real time. This is mainly important in the case of intrusion detection and prevention systems. Since supervised learning requires a large amount of labeled data that are not always be available, users can rely instead on semi-supervised algorithms. This type requires much less labeled data versus unlabeled data.

Moreover, machine learning can be used for the selection of the set of channels having the best conditions in a system with multiple links/channels. This is applicable in a Multiple-Input Multiple-Output or in multi-homed systems (mobile device with Wi-Fi and cellular connections). Following this step, users can utilize the chosen set for legitimate data transfer and the remaining links to send jamming signals to illegitimate users. One can also use machine learning to extract the unique features of the common channel between the legitimate entities and then, random nonce values can be derived and an encryption key can be constructed by combining the nonce with a secret key that is only know to the communicating entities. the resulting key can then be used to provide data confidentiality, privacy, authentication, and message integrity.

It should also be noted that current advances in hardware optimizations will reduce the associated delays and costs of some ML schemes that typically require high computational complexity and resources.

VII. Conclusion

In this overview, we summarized the different physical layer security schemes, in the literature, which employ machine learning algorithms to achieve robust security. The presented schemes have been thoroughly described and classified into three groups, each targeting a different security service including authentication, confidentiality and intrusion detection. These schemes were compared and assessed in terms of their advantages and limitations, and several recommendations were proposed. Our future work will focus on the design and implementation of a physical layer security scheme that employs machine learning efficiently for various security services.

References

[1] M. Xue, C. Yuan, H. Wu, Y. Zhang, and W. Liu, “Machine learning security: Threats, countermeasures, and evaluations,” *IEEE Access*, vol. 8, pp. 74 720–74 742, 2020.

[2] H. Noura, R. Melki, A. Chehab, and M. Mansour, “A physical encryption scheme for low-power wireless M2M devices: a dynamic key approach,” *Mobile Networks and Applications*, vol. 24, no. 2, pp. 447–463, 2019.

[3] H. Noura, R. Melki, A. Chehab, M. Mansour, and S. Martin, “Efficient and secure physical encryption scheme for low-power wireless M2M devices,” in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 1267–1272.

[4] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, “A survey on ofdm physical layer security,” *Physical Communication*, vol. 32, pp. 1–30, 2019.

[5] E. Alpaydin, *Introduction to machine learning*. MIT press, 2020.

[6] X. Zhang, “Machine learning,” in *A Matrix Algebra Approach to Artificial Intelligence*. Springer, 2020, pp. 223–440.

[7] M. Mohri, A. Rostamizadeh, and A. Talwalkar, *Foundations of machine learning*. MIT press, 2018.

[8] S. Dhankhad, E. Mohammed, and B. Far, “Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study,” in *IEEE International Conference on Information Reuse and Integration (IRI)*. IEEE, 2018, pp. 122–125.

[9] A. Munther *et al.*, “A preliminary performance evaluation of K-means, KNN and EM unsupervised machine learning methods for network flow classification,” *Int. J. Electr. Comput. Eng*, vol. 6, no. 2, p. 778, 2016.

[10] Y. Chen, X. Zhu, and S. Gong, “Semi-supervised deep learning with memory,” in *Proceedings of the European Conference on Computer Vision (ECCV)*, 2018, pp. 268–283.

[11] C. Wirth, R. Akrour, G. Neumann, and J. Fürnkranz, “A survey of preference-based reinforcement learning methods,” *The Journal of Machine Learning Research*, vol. 18, no. 1, pp. 4945–4990, 2017.

[12] H. Fang, X. Wang, and S. Tomasin, “Machine learning for intelligent authentication in 5g and beyond wireless networks,” *IEEE Wireless Communications*, vol. 26, no. 5, pp. 55–61, October 2019.

[13] F. Pan, H. Wen, R. Liao, Y. Jiang, A. Xu, K. Ouyang, and X. Zhu, “Physical layer authentication based on channel information and machine learning,” in *2017 IEEE Conference on Communications and Network Security (CNS)*, Oct 2017, pp. 364–365.

[14] J. Yoon, Y. Lee, and E. Hwang, “Machine learning-based physical layer authentication using neighborhood component analysis in mimo wireless communications,” in *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct 2019, pp. 63–65.

[15] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R. Liao, and J. Chen, “Threshold-free physical layer authentication based on machine learning for industrial wireless cps,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6481–6491, Dec 2019.

[16] H. Fang, X. Wang, and L. Hanzo, “Learning-aided physical layer authentication as an intelligent process,” *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2260–2273, March 2019.

[17] X. Qiu, Z. Du, and X. Sun, “Artificial intelligence-based security authentication: Applications in wireless multimedia networks,” *IEEE Access*, vol. 7, pp. 172 004–172 011, 2019.

[18] X. Qiu, T. Jiang, S. Wu, C. Jiang, H. Yao, M. H. Hayes, and A. Benslimane, “Wireless user authentication based on klt and gaussian mixture model,” in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2019, pp. 1–5.

[19] C. Pei, N. Zhang, X. S. Shen, and J. W. Mark, “Channel-based physical layer authentication,” in *2014 IEEE Global Communications Conference*, Dec 2014, pp. 4114–4119.

[20] B. Chatterjee, D. Das, S. Maity, and S. Sen, “Rf-puf: Enhancing iot security through authentication of wireless nodes using in-situ machine learning,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, Feb 2019.

[21] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile driver fingerprinting: A new machine learning based authentication scheme," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1417–1426, 2020.

[22] Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. Zhou, "The individual identification method of wireless device based on dimensionality reduction and machine learning," *The Journal of Supercomputing*, vol. 75, no. 6, pp. 3010–3027, 2019.

[23] S. Chen, H. Wen, J. Wu, A. Xu, Y. Jiang, H. Song, and Y. Chen, "Radio frequency fingerprint-based intelligent mobile edge computing for internet of things authentication," *Sensors*, vol. 19, no. 16, p. 3610, 2019.

[24] W. Lee and R. B. Lee, "Implicit smartphone user authentication with sensors and contextual machine learning," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017, pp. 297–308.

[25] B. Bezawada *et al.*, "IoTsense: Behavioral fingerprinting of IoT devices," *arXiv preprint arXiv:1804.03852*, 2018.

[26] S. Li, M. Cheng, Y. Chen, C. Fan, L. Deng, M. Zhang, S. Fu, M. Tang, P. Shum, and D. Liu, "Enhancing the physical layer security of ofdm-pons with hardware fingerprint authentication: a machine learning approach," *Journal of Lightwave Technology*, pp. 1–1, 2020.

[27] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "Iot sentinel: Automated device-type identification for security enforcement in iot," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2017, pp. 2177–2184.

[28] T. D. Nguyen, S. Marchal, M. Miettinen, N. Asokan, and A. Sadeghi, "Dïot: A self-learning system for detecting compromised iot devices," *CoRR, vol. abs/1804.07474*, 2018.

[29] S. Siby, R. R. Maiti, and N. Tippenhauer, "Iotscanner: Detecting and classifying privacy threats in iot neighborhoods," *arXiv preprint arXiv:1701.05007*, 2017.

[30] H. Kawai, S. Ata, N. Nakamura, and I. Oka, "Identification of communication devices from analysis of traffic patterns," in *2017 13th International Conference on Network and Service Management (CNSM)*. IEEE, 2017, pp. 1–5.

[31] A. Sivanathan, H. H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Classifying iot devices in smart environments using network traffic characteristics," *IEEE Transactions on Mobile Computing*, 2018.

[32] L. Bai, L. Yao, S. S. Kanhere, X. Wang, and Z. Yang, "Automatic device classification from network traffic streams of internet of things," in *2018 IEEE 43rd Conference on Local Computer Networks (LCN)*. IEEE, 2018, pp. 1–9.

[33] S. Sciancalepore, O. A. Ibrahim, G. Oligeri, and R. Di Pietro, "Picking a needle in a haystack: Detecting drones via network traffic analysis," *arXiv preprint arXiv:1901.03535*, 2019.

[34] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, and B. Preneel, "Physical-layer fingerprinting of lora devices using supervised and zero-shot learning," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2017, pp. 58–63.

[35] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi, and A. S. Uluagac, "Peek-a-boo: I see your smart home activities, even encrypted!" *arXiv preprint arXiv:1808.02741*, 2018.

[36] B. Copos, K. Levitt, M. Bishop, and J. Rowe, "Is anybody home? inferring activity from smart home network traffic," in *2016 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2016, pp. 245–251.

[37] J. Ortiz, C. Crawford, and F. Le, "Devicemien: network device behavior modeling for identifying unknown iot devices," in *Proceedings of the International Conference on Internet of Things Design and Implementation*. ACM, 2019, pp. 106–117.

[38] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "A machine learning based framework for IoT device identification and abnormal traffic detection," *Transactions on Emerging Telecommunications Technologies*, p. e3743, 2019.

[39] W. Yan, L. K. Mestha, and M. Abbaszadeh, "Attack detection for securing cyber physical systems," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8471–8481, Oct 2019.

[40] R. Li, Q. Duan, J. Xue, S. Zhang, and C. He, "A directional reactive jamming scheme based on machine learning," in *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*, Oct 2019, pp. 1–5.

[41] A. Sargolzaei, C. D. Crane, A. Abbaspour, and S. Noei, "A machine learning approach for fault detection in vehicular cyber-physical systems," in *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Dec 2016, pp. 636–640.

[42] Z. Weisha, S. Jinguang, and L. Jiazhong, "Machine learning-based system electromagnetic environment anomaly detection method," in *2018 International Conference on Smart Grid and Electrical Automation (ICSGEA)*, June 2018, pp. 115–117.

[43] G. Prasad, Y. Huo, L. Lampe, and V. C. M. Leung, "Machine learning based physical-layer intrusion detection and location for the smart grid," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Oct 2019, pp. 1–6.

[44] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2018.

[45] C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, and M. Furdek, "Experimental study of machine-learning-based detection and identification of physical-layer attacks in optical networks," *Journal of Lightwave Technology*, vol. 37, no. 16, pp. 4173–4182, Aug 2019.

[46] E. Unal, S. Sen-Baidya, and R. Hewett, "Towards prediction of security attacks on software defined networks: A big data analytic approach," in *2018 IEEE International Conference on Big Data (Big Data)*, Dec 2018, pp. 4582–4588.

[47] A. Albehadili, A. Ali, F. Jahan, A. Y. Javaid, J. Oluochy, and V. Devabhaktuniz, "Machine learning-based primary user emulation attack detection in cognitive radio networks using pattern described link-signature (pdls)," in *2019 Wireless Telecommunications Symposium (WTS)*, April 2019, pp. 1–7.

[48] Y. Yengi, A. Kavak, H. Arslan, K. Küçük, and H. Yiğit, "Malicious relay node detection with unsupervised learning in amplify-forward cooperative networks," in *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Sep. 2019, pp. 1–5.

[49] M. Hachimi, G. Kaddoum, G. Gagnon, and P. Illy, "Multi-stage jamming attacks detection using deep learning combined with kernelized support vector machine in 5G cloud radio access networks," *arXiv preprint arXiv:2004.06077*, 2020.

[50] J. Xing, T. Lv, and X. Zhang, "Cooperative relay based on machine learning for enhancing physical layer security," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2019, pp. 1–6.

[51] D. He, C. Liu, T. Q. S. Quek, and H. Wang, "Transmit antenna selection in mimo wiretap channels: A machine learning approach," *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 634–637, Aug 2018.

[52] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6522–6530, Dec 2019.

[53] F. Kriebel, S. Rehman, M. A. Hanif, F. Khalid, and M. Shafique, "Robustness for smart cyber physical systems and internet-of-things: From adaptive robustness methods to reliability and security for machine learning," in *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, July 2018, pp. 581–586.

[54] Z. Deng, Q. Sang, Y. Gao, and C. Cai, "Optimal relay selection for wireless relay channel with external eavesdropper: a nn-based approach," in *2018 IEEE/CIC International Conference on Communications in China (ICCC)*, Aug 2018, pp. 515–519.

[55] J. Zhou, S. Zheng, X. Yu, X. Jin, and X. Zhang, "Low probability of intercept communication based on structured radio beams using machine learning," *IEEE Access*, vol. 7, pp. 169 946–169 952, 2019.

[56] M. Shafique, F. Khalid, and S. Rehman, "Intelligent security measures for smart cyber physical systems," in *2018 21st Euromicro Conference on Digital System Design (DSD)*, Aug 2018, pp. 280–287.

[57] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 2595–2621, Fourthquarter 2018.

[58] F. Hussain, R. Hussain, S. Hassan, and E. Hossain, "Machine learning in IoT security: current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, 2020.

[59] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for internet of things," *International Journal of Machine Learning and Cybernetics*, vol. 9, no. 8, pp. 1399–1417, 2018.