Seamless Wireless Communication Platform for Internet of Things Applications

Venkataramani Kumar, *Student Member, IEEE,* Jiahui Yu, *Student Member, IEEE,* Fuhao Li, *Student Member, IEEE,* Jielun Zhang, *Student Member, IEEE,* Feng Ye, *Senior Member, IEEE,* Sanjeevi Karri and Guru Subramanyam, *Senior Member, IEEE*

Abstract

The rapid growth of the Internet of Things (IoT) devices resulted in the proliferation of wireless technologies to cater to their increasing data rate requirements and support multiple applications. However, such ever-increasing wireless technologies present numerous challenges such as incompatible wireless standards, increased energy consumption, and insecure communication. The traditional gateways proposed in the literature suffers from limitations such as computational complexity, resource requirements, increased cost, and device size. We vision an era of seamless wireless communication to alleviate the aforementioned challenges in IoT applications. through three inter-dependent functionalities namely detection and identification of wireless technologies, energy-efficient transmit power control, and secure end-to-end communication. To prove the concept, a new gateway is proposed to achieve these three functionalities with only physical layer measurements so that the different communication protocols in the higher layers can be avoided. Novel schemes are conceptualized for resource-limited seamless IoT applications. Moreover, the conceptual seamless IoT platform is validated through software-based computer simulation and software-defined radio-based testbed implementation. The preliminary analysis demonstrates that the proposed platform has great potential in advancing seamless IoT applications.

Index Terms

Internet of Things (IoT); seamless wireless communications; gateway

Venkataramani Kumar, Jiahui Yu, Fuhao Li, Jielun Zhang and Feng Ye are with the Department of Electrical and Computer Engineering, University of Dayton, Dayton, OH, USA. E-mail: {yuj016, tiruchirappallinarv1, lif003, zhangj46, fye001}@udayton.edu. Venkataramani Kumar and Jiahui Yu contributed equally.

Sanjeevi Karri and Guru Subramanyam are with Prixarc LLC., Dayton, OH, USA E-mails: {sanjeevi,guru}@prixarc.com.

I. Introduction

The exponential growth of IoT devices modernized our lives and society. It is estimated that the number of IoT devices will touch nearly 30.9 billion by the end of 2025 [1]. This will lead to the proliferation of wireless technologies to new applications like smart systems that modernize our lives and society. However, such an exponential development of wireless technologies brings multiple challenges. First, compatibility becomes an issue among different wireless standards. The devices in the heterogeneous network operate on various standards, such as IEEE 802.11 (Wi-Fi), 802.15.1 (Bluetooth), and IEEE 802.15.4 (Zigbee). In the current smart home market, we have devices like Hue smart bulb supported by Zigbee. However, we need an extra bridge supporting both Zigbee and Bluetooth to enable remote controls on phones. Also because of the development of different wireless technologies and their different performance in many areas like power consumption, data transmission rate, etc., mixed-use of these wireless technologies will be trending. It is imperative to ensure seamless communication across IoT devices with various wireless technologies. Second, the limited spectrum resources result in increased competition amongst wireless technologies. Third, most of the IoT devices operate on the same spectrum, e.g., the industrial, scientific and medical (ISM) band [2], which may introduce interference to different devices. Fourth, it is imperative to ensure that the system is robust to changing environmental conditions and security threats regardless of communication technologies. Failure to address the limitations above thwarts the development of IoT. Traditionally, gateways are used to entrench indirect communication among heterogeneous IoT devices by bridging different wireless technologies. There is usually one device that supports two different standards and serves as the transit for different devices. For example, we need a bridge to connect to a smartphone through Bluetooth, and the bridge will connect to smart bulbs through ZigBee, so through the bridge, we can use our phones to control the bulb. Some researchers also proposed other methods to solve the gap in different communication standards. Authors in [3] provided Zigbee-Bluetooth Low Energy (BLE) gateway to manage and control home appliances. Cross-technology communication [2] ensures direct communication among different wireless technologies. However, these approaches may not fully support seamless IoT applications as the wireless technologies are considered and assumed known beforehand. Moreover, these existing approaches did not address some of the important issues in seamless IoT communications, such as security and energy efficiency. In our proposed seamless IoT platform, we will have one or multiple devices serve as the transit. Different from traditional gateways, we also provide performance in communication, power consumption, and security.

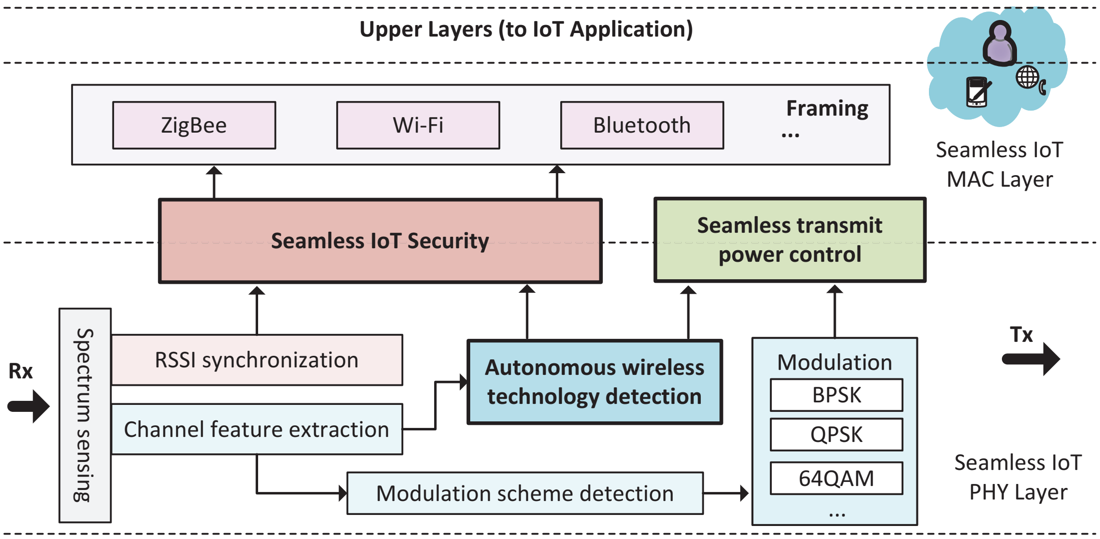


Fig. 1: Conceptual platform for Seamless IoT communications.

In this paper, we vision a concept of seamless wireless communication to address the limitations discussed above. As shown in Fig. 1, the conceptual platform consists of three major modules, i.e., autonomous wireless technology detection, seamless IoT security, and seamless transmit power control. Detecting the wireless technology would be the key to achieving seamless IoT transmissions. The proposed autonomous wireless technology detection module in the seamless IoT communication platform conducts the detection based on the extracted physical (PHY)-layer channel features such as received signal strength indicator (RSSI), symbol levels, bandwidth, and modulation schemes. Note that we use the physical attributes to detect different wireless technologies, and the detection can be easily extended for any wireless technology. Considering different modulations can help our autonomous wireless technology detection cover future wireless technologies. For example, Wi-Fi 5 uses 256-quadrature amplitude modulation (QAM) while Wi-Fi 6 uses 1024-QAM. Detecting the modulation scheme instead of adding new modules for new technologies can enable new technology detection. Meanwhile, security is an equally critical aspect in IoT applications [4]. To avoid inconsistency of security protocols in the higher layers of different wireless communication technologies, the proposed security control module provides security features across different wireless communication technologies mainly through PHY-layer processes. Energy efficiency is also studied as it is a crucial aspect of seamless IoT applications [5]. The power control module optimizes the transmit power of the IoT devices to ensure energy efficiency across different wireless communication technologies. It is also worth mentioning that new schemes are derived with preliminary testbed implementation to prove the concept of seamless wireless communication, which are illustrated in the following sections.

II. Autonomous Wireless Technology Detection

In general, existing wireless technology extraction approaches can be mainly classified into two different categories, namely medium access control (MAC)-layer and PHY-layer methods [6]. MAC-layer methods explore signatures of MAC-layer features, e.g., frame inter-arrival time, frame length, etc. However, MAC-layer methods would assume prior knowledge on targeting wireless technologies, which can be limited or unknown to seamless IoT applications. PHY-layer methods involve the use of spectrum measurements that could be available to most wireless technologies in seamless IoT applications. In the proposed concept illustrated in Fig. 2, the wireless technology detection is achieved in real-time by a machine learning based classifier given the PHY-layer channel features.

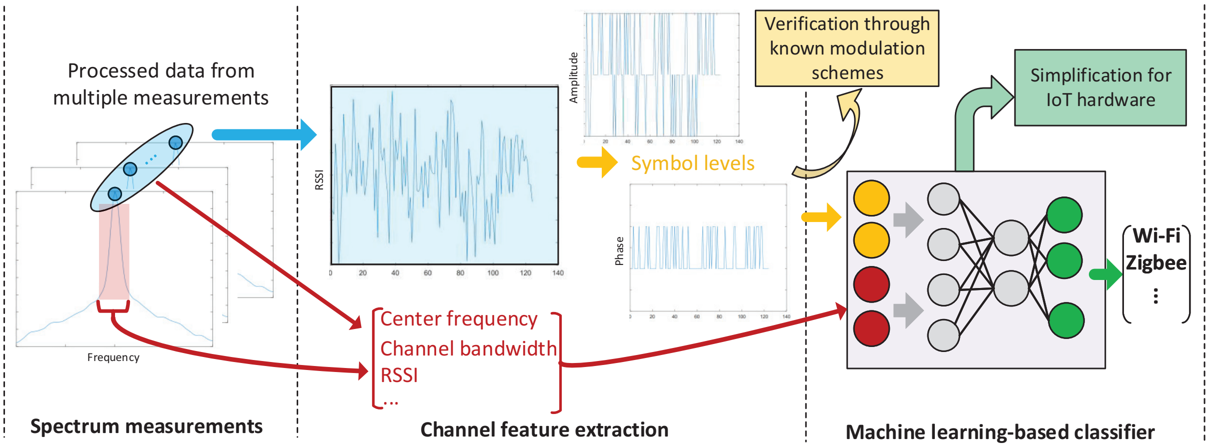

Processed data from multiple measurements
Frequency
Spectrum measurements
RSSI
0 20 40 60 80 100 120 140
Amplitude
Symbol levels
Phase
Center frequency
Channel bandwidth
RSSI
...
Channel feature extraction
Verification through known modulation schemes
Simplification for IoT hardware
Wi-Fi
Zigbee
⋮
Machine learning-based classifier

Fig. 2: Autonomous wireless technology detection.

A. *Basic Channel Feature Extraction*

A straightforward PHY-layer measurement can be the In-phase and Quadrature-phase (I/Q) data [6]. Various basic channel features can be detected from the I/Q measurements, including RSSI, center frequency, channel bandwidth, etc. For example, the center frequency can be estimated at where the highest RSSI is from the spectrum scan. The bandwidth can be estimated based on the center frequency by finding the higher and lower frequencies where the RSSI values have a, e.g., 3 or 6-decibel drop from that of the center frequency. Arguably speaking, different wireless technologies may have a unique combination of PHY-layer channel features. For example, a typical Wi-Fi transmission could have a higher RSSI and a wider channel bandwidth than a Zigbee transmission. However, depending on the PHY-layer measurement and practical configurations, any individual of such channel features, may not distinguish a wireless technology.

B. *Symbol Level Extraction and Modulation Scheme Detection*

Besides the basic channel features, modulation schemes can be a decisive feature for wireless technology detection. Multiple modulation scheme detection approaches proposed in existing literature can be categorized into decision-theoretic and feature-based approaches [7]. The decision-theoretic approaches, e.g., the maximum likelihood-based approaches, present the classification to be a hypothesis problem. Although such approaches reduce classification errors, they introduce high computational complexity and are non-robust to unknown channel conditions. The feature-based approaches require expertise in the fields to extract the features that contribute significantly to the classification process. Manual extraction of features is tedious and costly in both time and resources. Besides, finding the exact modulation scheme may not be required to detect the wireless technologies. Instead, we propose to estimate symbol levels from the I/Q measurements. For example, binary phase-shift keying (BPSK) should return two distinct phase levels and one amplitude level. The combination of the symbol levels would be unique to a specific modulation scheme. Using the symbol levels instead of the actual modulation schemes can be advantageous in two ways. First, the symbol level extraction is a future-proof process, regardless of new and added modulation schemes in new wireless technologies. For example, 1024-QAM is supported in Wi-Fi 6, but Wi-Fi 5 only supports 256-QAM. Second, the overall processing complexity can be reduced as the classification is unnecessary. Nonetheless, a classifier can still be developed to validate the extracted symbol levels using known modulation schemes. The exact modulation schemes may also be needed in seamless IoT communications once the wireless technology is detected.

C. Machine Learning based Wireless Technology Detection

Machine learning is a subfield of artificial intelligence (AI), and it has gradually been introduced to wireless technology detection [6]. However, existing schemes mainly rely on raw PHY-layer measurements, e.g., RSSI, which can be abundant and perhaps noisy when developing a classifier for identifying wireless technologies. Those classifiers may result in a complex structure due to the raw PHY layer characteristics. The machine learning-based classifier in the proposed seamless IoT platform is to be constructed with a simple structure so that an IoT device with limited computing capability can execute the detection process in real-time. Given the fact that the PHY-layer channel features, including the basic channel features and the modulated symbol levels, are extracted from raw measurements, the classifier would only need to process a low-dimensional input. Therefore, the classifier can be implemented with a simple structure that prioritizes computational efficiency on a seamless IoT device. Complex models, e.g., deep learning-based classifiers, would be over-complicated and resource-hungry for seamless IoT devices. However, an extensive training dataset is usually required for classifier initialization and maintenance. As a result, the classifier should be developed and managed using advanced computing platforms, e.g., on workstations or high-performance cloud computing servers. With the classifier well developed, it may be further simplified to more efficient functions on an IoT processing unit. A dedicated processor for machine learning may further benefit the classifier implementation.

III. PHY-Layer Supported Seamless IoT Security

A. Overview of the PHY-Layer Supported Seamless IoT Security

PHY-layer security for IoT has attracted increasing attention recently [8, 9]. However, the existing PHY-layer security methods may not be applied directly in a seamless IoT scenario due to the limited support in security. The security issue in the proposed seamless IoT concept will be studied by leveraging the existing MAC-layer security features while exploiting additional functions from PHY-layer security. The security features provided by PHY-layer security need to compensate for the inconsistency across different wireless technologies. For example, device authentication is not provided for Zigbee communications at the same level as Wi-Fi communications. Without opportunistic wireless encryption, data encryption may not be provided for open Wi-Fi communications. Moreover, access control may be unavailable in the current wireless technologies such as Zigbee and Bluetooth to accommodate large-scale and dynamic IoT scenarios. Therefore, the major security features to be provided by PHY-layer security are authentication, access control, and confidentiality. PHY-layer security can also be used to generate and distribute domain secret parameters to support the MAC-layer cryptographic algorithms, e.g., the advanced encryption standard (AES).

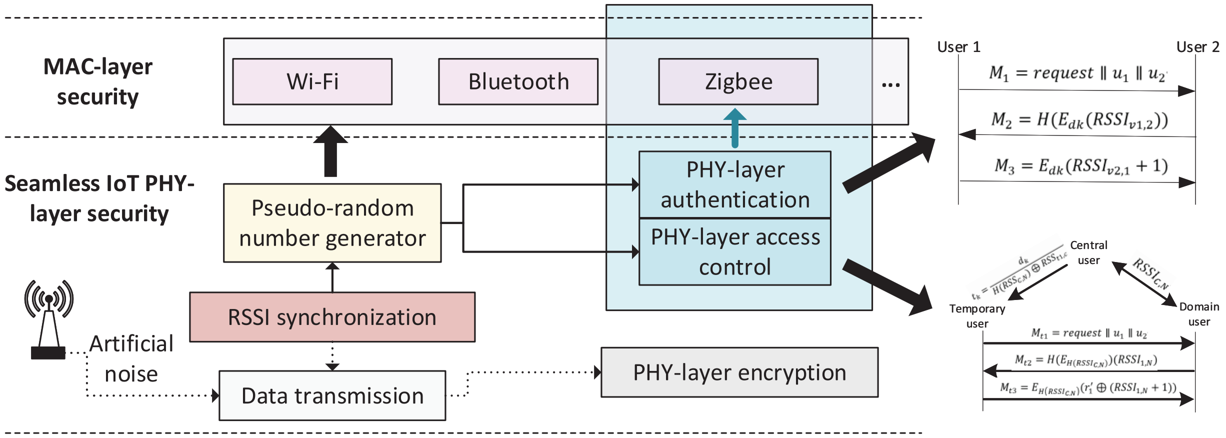

MAC-layer security
Wi-Fi
Bluetooth
Zigbee
...
Seamless IoT PHY-layer security
Pseudo-random number generator
PHY-layer authentication
PHY-layer access control
RSSI synchronization
Artificial noise
Data transmission
PHY-layer encryption
User 1
User 2
$M_1 = request \parallel u_1 \parallel u_2$
$M_2 = H(E_{dk}(RSSI_{v1,2}))$
$M_3 = E_{dk}(RSSI_{v2,1} + 1)$
Central user
$t_k = \frac{d_k}{H(RSS_{C,N}) \oplus RSS_{t1,C}}$
$RSSI_{C,N}$
Temporary user
Domain user
$M_{t1} = request \parallel u_1 \parallel u_2$
$M_{t2} = H(E_{H(RSSI_{C,N})})(RSSI_{1,N})$
$M_{t3} = E_{H(RSSI_{C,N})}(r_1' \oplus (RSSI_{1,N} + 1))$

Fig. 3: Overview of the PHY-layer supported seameless IoT security.

B. PHY-Layer Authentication

PHY-layer security exploits the unique and synchronous information, e.g., RSSI, between two wireless devices. Generally, a third device cannot receive the same RSSI if it is more than half of the wavelength away from the legitimate users [10]. We propose to achieve PHY-layer authentication based on RSSI synchronization and a group certification process. Note that the authentication is limited to two known devices within the same IoT network. The initial deployment is beyond the scope of the proposed security features of seamless IoT communications. Suppose a seamless IoT network contains a few IoT devices, one of the trusted IoT devices that are non-intrusive will be chosen randomly and appointed as the central server for the group certificate generation. The central node broadcasts an initialization request and synchronizes a unique RSSI with each IoT device. The group certificate is then computed from all the synchronized RSSI values by adding all the values or generating a hash value accordingly. The group certificate can be transmitted to each user through a secure channel via either the MAC or PHY layers (to be discussed later in this section). The IoT devices then use the certificate to prove their legitimacy in the network domain. For example, mutual authentication can be achieved between any two IoT devices by first synchronizing the current RSSI and then validation using the certificate, e.g., exchanging the summation of the certificate and the current RSSI. The actual implementation may vary depending on whether the authentication is processed before or after the detection of the corresponding wireless technology. Once authenticated, the identities of the devices, e.g., MAC addresses, will be linked to the corresponding physical-layer information, i.e., the group certificate in the prior description.

C. PHY-Layer Access Control

A straightforward way to add a new IoT device is to initialize the whole network and regenerate the group certificate. However, it may be less efficient in a dynamic environment where frequent device adding or removal requests are issued. In this regard, the current central device and the targeting IoT devices will generate a temporary session key and assign the key to the device. Unlike regenerating the group certificate, the temporary session key generation only needs the participation of the controller, the new device, and the devices it wants to communicate with. While the secret values would be derived from the RSSI values between the participants, the temporary session key generation would require running the cryptographic algorithms in the MAC layer, which means the participants must have agreed on MAC-layer protocols, e.g., via the autonomous wireless technology detection.

D. PHY-Layer Encryption

PHY-layer encryption can be most useful when seamless IoT devices are unaware of wireless technologies or the MAC-layer security protocols. In this manner, the PHY-layer encryption would require the assistance of artificial noises. If the artificial noises can be fully synchronized between the two legitimate users, the distorted signal can be recovered on both sides by eliminating the artificial noises. Another possible approach is to tune the power of artificial noises so that the legitimate users can still have a good enough signal-to-noise ratio (SNR) to recover all transmissions, while attackers cannot reach the threshold of SNR to fully recover the signals.

In practice, the latter option could be easier to deploy since the synchronization of artificial noise could be challenging. However, proper modeling and evaluation of eavesdroppers would be required to optimize the power of artificial noise.

E. PHY-Layer Supported Domain Secret for MAC-Layer Cryptographic Algorithms

While the PHY-layer security can provide some security features, it may not be the most efficient implementation for seamless IoT communications. Moreover, the IoT devices may not support all the advanced functions required for the PHY-layer security protocols. Therefore, the proposed seamless IoT PHY-layer security mainly focuses on providing domain secret values for MAC-layer cryptographic algorithms. Although the MAC-layer security protocol of each wireless technology may have defined the key agreement, the secret keys for the same algorithm, e.g., AES, would not be the same for two different technologies, e.g., Wi-Fi and Zigbee, running on the same IoT device. Moreover, the secret key generation and distribution protocols are not equally defined across different wireless technologies. For example, Zigbee may not have the same key refresh rate as Wi-Fi. To address these issues, we propose to generate and distribute the secret values, e.g., keys to AES, based on the RSSI value synchronized in the PHY layer. Our preliminary testbed implementation shows that an RSSI could remain unchanged for 1-2 ms if a 5-bit value is needed. The preliminary analysis uses the PHY-layer settings of a Zigbee transmission on a software-defined radio (SDR) platform. In this manner, exchanging a 128-bit secret value would introduce a noticeable delay in the transmission. To address this issue, the secret value may be exchanged once during the initialization process and generate a fixed-size output using a pseudo-random number generator with an incremental counter. Note that the wireless technology may not be confirmed before generating the secret values.

IV. Seamless Transmit Power Control

Existing approaches to achieve energy efficiency focus more on a single wireless technology. For example, authors in [11] analyzed various possibilities, such as the use of reduced network topology at the same time while preserving connectivity and coverage. However, most existing techniques promote energy efficiency in devices operating with one wireless technology. In the proposed concept, the seamless transmit power control relies on wireless technology detection. The transmit power of a seamless IoT can be adjusted to balance the transmission data rate and the power consumption for optimal energy efficiency.

In our prior work, a game-theoretical approach was developed to optimize the power control of different wireless technologies in a seamless IoT communication scenario [12]. In the demonstrating scenario, a seamless IoT device may operate either Wi-Fi or Zigbee in the same spectrum. The game-theoretical approach is to achieve the equilibrium that maximizes the energy efficiency defined as the ratio of data rate to power consumption for the chosen wireless technology. In the testbed implementation, the IoT devices are assumed unaware of the transmission technologies of the other devices, and thus cannot exchange the power control settings via digital transmissions. A practical scheme was developed so that each IoT device may sense the action of increase or decrease of transmit power by measuring the RSSI as a signal. For example, a relatively high RSSI measurement indicates that the transmit power increase, while a relatively low RSSI measurement indicates the opposite action. With a step size pre-defined for each increase or decrease, an equilibrium can be approximated after a few of the signaling processes.

V. Preliminary Testbed Implementation and Evaluations

Preliminary scheme designs and testbed implementation have been conducted to partially demonstrate the concept of a seamless wireless communication platform for IoT applications [12, 13]. For ease of illustration, the testbed shown in this work comprises three laptop computers connected to USRP SDR boards. The testbed includes two transmitters emulating two different wireless technologies, i.e., Wi-Fi and Zigbee, respectively. A third SDR is a standalone device that executes the seamless IoT schemes, i.e., the autonomous wireless technology detection, optimal power control, and RSSI exchange for PHY-layer security. It would be straightforward to modify all SDR boards to operate as seamless IoT devices. Note that the B200 and B210 boards were used identically in the implementation.

We take the advantage of the programmable SDR boards to customize frequency, bandwidth, modulation, etc. The main contribution of our paper is autonomous wireless technology detection and the seamless IoT platform. After detection, testing BER, throughput, and other parameters of the detected wireless technology will be the same as testing the. It is also beyond our scope of work to include the information of all the wireless technologies since all different wireless technologies have different BER, throughput, and power consumption. Since there are many wireless technologies and researchers keep developing new technologies, implementing different modules will be difficult and time-consuming. For example, Wi-Fi 5 uses 256-QAM and Wi-Fi 6 supports 1024-QAM. Although the SDR board is overpowered regarding our needs, using

SDR is a more efficient way compared to deploying different modules. Once the seamless IoT platform is completed, we will use cheaper boards and modules to lower the cost and realize the same functions. Details of the settings used in the evaluation are given in TABLE I.

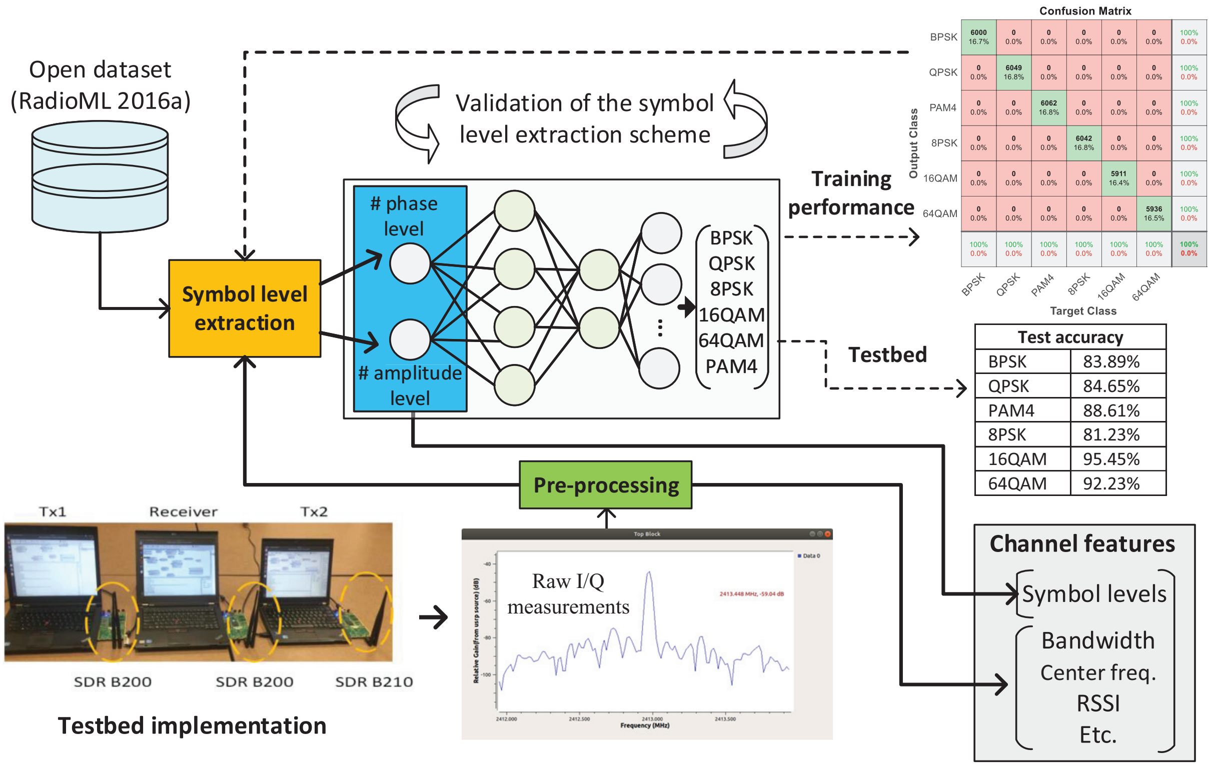
TABLE I: Settings for the testbed implementation and evaluations.

Settings for evaluating the basic channel feature extraction			
Device	Transmitter 1	Transmitter 2	Receiver
Sampling frequency	1 MHz	128 KHz	4 MHz
Bandwidth	500 KHz	64 KHz	2 MHz
Center frequency	2.413 GHz		2.412 GHz
Gain (normalized)	0.75		0.65
Settings for evaluating symbol level extraction and modulation detection			
Settings for SDR implementation			
Devices	Transmitter	Receiver	
Center frequency	2.412 GHz	2.412 GHz	
Bandwidth	4 MHz	4 MHz	
Block size	144	144	
Gain (normalized)	0.45	0.75	
# Samples	120,000		
# Training samples	100,000		
# Testing samples	20,000		
Selected data from the RadioML 2016.10a open dataset			
Modulation	BPSK, QPSK, 8PSK, 16-QAM, 64-QAM,PAM4		
Feature dimension	2 × 128		
SNR range	-20 dB to 20 dB		
# Samples (per class)	20,000		
# Training samples (per class)	14,000		
# Testing samples (per class)	6,000		
Settings for the multi-layer perceptron-based modulation classifier			
Inputs	Amplitude and phase levels (symbol levels)		
Layers	Input, Hidden (2) and classification		

Activation function	ReLU		
Settings for wireless technology detection			
Settings for SDR testbed emulations			
Device	Wi-Fi Tx	Zigbee Tx	Receiver
Center frequency	2.412 GHz	2.412 GHz	2.412 GHz
Bandwidth	500 KHz	64 KHz	2 MHz
Sampling frequency	1 MHz	128 KHz	4 MHz
Gain (normalized)	0.75	0.75	0.65
Modulation	BPSK	QPSK	NA
Sample length	144	144	144
Duration of operation	2-minute cycle		Continuously
# Samples (per technology)	50,000		
# Training samples	40,000 per technology (plus noise from idle cycle)		
# Testing samples	10,000 per technology (plus noise from idle cycle)		
Settings for the Multilayer Perceptron based classifier			
Inputs	Extracted basic channel features and symbol levels		
Layers	Input, hidden (2) and classification layers		
Activation function	ReLU		

A. Demonstration of Basic Channel Feature Extraction

Initially, a seamless IoT device scans the spectrum and gathers the raw I/Q measurements. As indicated in Fig. 4, some of the basic channel features such as center frequency and bandwidth can be extracted straightforwardly from the RSSI measurements. Practical implementations may require multiple scans to cover the entire spectrum of different wireless communication technologies, as well as to improve the accuracy of estimation in a noisy wireless environment for IoT applications. In our demonstration, multiple measurements are taken due to the bandwidth limitation of the SDR equipment. Note that the estimates could still be off from the actual settings due to dynamic wireless environments after the post-processing. Nonetheless, differences in bandwidth and average RSSI can be easily spotted between the measurements from two different wireless technologies, i.e., Wi-Fi and Zigbee. Such differences would distinguish the channel features and contribute to the machine learning supported classifier development.



Confusion Matrix

Output Class	BPSK	QPSK	PAM4	8PSK	16QAM	64QAM	
BPSK	6000 16.7%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
QPSK	0 0.0%	6049 16.8%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
PAM4	0 0.0%	0 0.0%	6062 16.8%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
8PSK	0 0.0%	0 0.0%	0 0.0%	6042 16.8%	0 0.0%	0 0.0%	100% 0.0%
16QAM	0 0.0%	0 0.0%	0 0.0%	0 0.0%	5911 16.4%	0 0.0%	100% 0.0%
64QAM	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	5936 16.5%	100% 0.0%
	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%

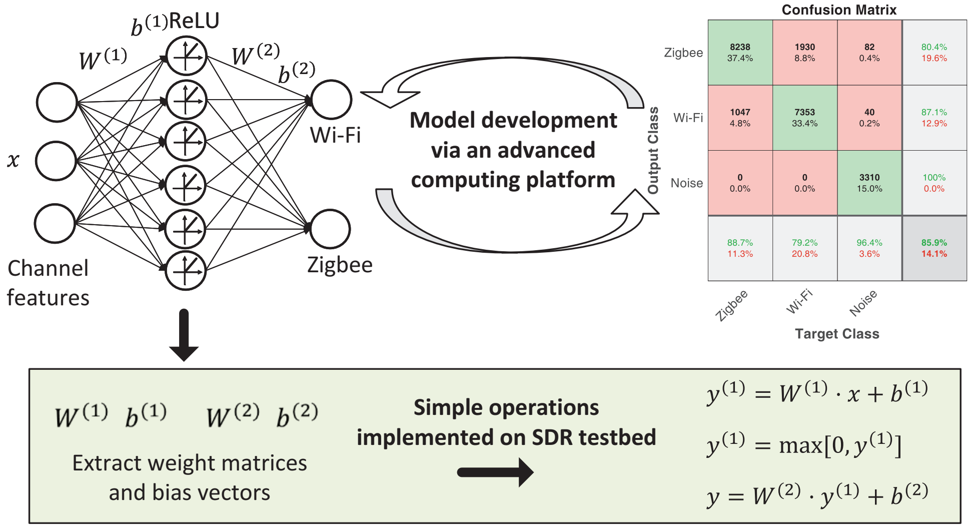
Target Class

Test accuracy	
BPSK	83.89%
QPSK	84.65%
PAM4	88.61%
8PSK	81.23%
16QAM	95.45%
64QAM	92.23%

Fig. 4: Preliminary testbed implementation on the channel feature extraction and modulation scheme detection.

B. Demonstration of Symbol Level Extraction and Modulation Scheme Detection

Aside from the channel features extracted from the initial process, modulation schemes can be detected from the raw I/Q measurements, e.g., using the symbol level extraction scheme developed in our prior work [13]. The scheme design and validation were first conducted using the open dataset RadioML 2016.10a [14] on 6 modulation schemes, i.e., BPSK, quadrature PSK (QPSK), pulse amplitude modulation 4-level (PAM4), 8-PSK, 16-QAM, and 64-QAM. Given the nature of the chosen modulation schemes, the symbol levels are defined as the number of amplitudes and number of phases. For example, BPSK should have one amplitude level and two phase levels, while QPSK should have one amplitude level and four phase levels. Due to the imperfect signals and incomplete information, the extracted symbol levels are not perfect. For example, the number of amplitudes could be one or two for BPSK, while the number of phase levels could be two or three in the meantime. Albeit such imperfection, we argue that the extracted symbol levels represent the corresponding modulation schemes. Specifically, a classifier was developed based on a multi-layer perceptron network, where the input features are the two symbol levels and the output is one of the six modulation schemes. The classifier can achieve perfect identification accuracy when using the open dataset. Meanwhile, the detection accuracy of the classifier is above 87% using the testbed measurements from spectrum scanning. The classification errors in the testbed implementations could be from the noises collected from the testbed implementation and inconsistent labels afterward. Note that the modulation classifier can be developed and updated offline if the dataset is updated with more modulation schemes. Nonetheless, the implementation of symbol level extraction would stay unchanged at the device level.


$b^{(1)}$ReLU
$W^{(1)}$
$W^{(2)}$
$b^{(2)}$
x
Wi-Fi
Zigbee
Channel features
Model development via an advanced computing platform
Confusion Matrix
Output Class
Target Class
$W^{(1)}$ $b^{(1)}$ $W^{(2)}$ $b^{(2)}$
Extract weight matrices and bias vectors
Simple operations implemented on SDR testbed
$y^{(1)} = W^{(1)} \cdot x + b^{(1)}$
$y^{(1)} = \max[0, y^{(1)}]$
$y = W^{(2)} \cdot y^{(1)} + b^{(2)}$

	Zigbee	Wi-Fi	Noise	
Zigbee	8238 37.4%	1930 8.8%	82 0.4%	80.4% 19.6%
Wi-Fi	1047 4.8%	7353 33.4%	40 0.2%	87.1% 12.9%
Noise	0 0.0%	0 0.0%	3310 15.0%	100% 0.0%
	88.7% 11.3%	79.2% 20.8%	96.4% 3.6%	85.9% 14.1%

Fig. 5: Classifier development and testbed implementation on wireless technology detection.

C. Machine Learning-based Wireless Technology Detector

Since the channel features and the symbol levels extracted from the spectrum measurements are merely a few inputs, the wireless technology detector can be developed as a simple-structured machine-learning classifier. For example, the demonstration in this work is based on a shallow-layer neural network with a single number of nodes in each hidden layer. The classifier was developed using a dataset collected from the testbed implementation by setting the transmitter as Wi-Fi, Zigbee, and idle. As illustrated in Fig. 5, the detection accuracy of Wi-Fi and Zigbee are around 80% or higher, while the detection accuracy of noise (or idle) is close to 100%. The misdetection could be from the imperfect labeling as the generic seamless IoT receiver may record noisy I/Q measurements due to the asynchronous settings from the transmitter. Better results may be achieved if the transmitter and the receiver are set to the same wireless technology during data collection and labeling. Due to the limited computing capability of IoT devices, even a shallow neural network could be too complicated for real-time processing. To improve the efficiency, the machine learning based classifier is implemented with simple functions such as addition and shifting on the SDR board. In this paper, the proof of concept is conducted using a powerful workstation and an open-source machine learning platform, i.e., PyTorch.

VI. Future Research Direction

The future research directions in seamless IoT communication are fourfold. First, the scheme design on wireless technology detection needs to be extended to prove more wireless technologies and communication channels. For example, the current Wi-Fi used in IoT devices may use triple bands in the 2.4 GHz and the 5 GHz spectrum. The next-generation Wi-Fi may exploit the 6 GHz spectrum and present different PHY-layer features [15]. In this case, the PHY-layer measurements need to have a wider spectrum coverage, e.g., by using an ultra-wideband antenna and/or with a universal protocol for multiple access. Moreover, the definition of symbol levels needs to be refined and comprehensive on top of the scheme design given in our prior work. Although the concept of symbol level extraction is future proof of new modulation schemes, it should be refined and validated frequently when a new wireless technology is adopted by a seamless IoT device. Second, the PHY-layer supported security needs to be explored further. For example, more efficient and robust RSSI synchronization is needed for faster secret generation and distribution between seamless IoT devices. New schemes and practical implementations need to be addressed for artificial noise management for PHY-layer encryption in a seamless communication environment with various wireless technologies. Moreover, other security features may be developed for PHY-layer only implementation in addition to the mutual authentication and access control for temporary users discussed in this work. Third, the system implementation of the schemes and algorithms needs to be optimized to accommodate the relatively low computing capability of IoT devices. In addition, a hardware-accelerated processing unit, e.g., an AI chip, may be required to execute machine learning algorithms for optimal power efficiency and real-time seamless IoT communications. Fourth, after getting implementation done on the USRP SDR boards, we will try to use other cheaper development boards like Respberry Pi to lower the cost. We will aim to lower the hardware cost, since no complicated calculation will be needed.

Besides the challenges mentioned above, the seamless IoT communication standardization would better guide and accelerate technology development.

VII. Conclusion

Due to the lack of standards, and inherent limitations in the existing gateways seamlessly connecting IoT devices from different manufacturers can be challenging in practice. In this paper, a new seamless communication platform was conceptualized for seamless, secure, and energy-efficient IoT communications between different IoT devices supported by various wireless technologies. The proposed seamless IoT platform is to achieve autonomous detection and switching among different wireless technologies, with the optimal energy efficiency that balances transmit power consumption and the communication requirements, and robust security protection across various wireless technologies. Preliminary schemes were designed to demonstrate the concept for basic feature extraction, symbol level extraction, modulation scheme detection, autonomous wireless detection, and power control. Nonetheless, the seamless IoT concept still has a few challenges, especially in more robust security protocol design and simplification of hardware implementation.

Acknowledgment

This project was supported by the U.S. Department of Energy (DOE) through Prixarc, LLC under Contract No. DE-SC0018617.

References

[1] I. Analytics, "Internet of things (iot) and non-iot active device connections worldwide from 2010 to 2025 (in billions)," 2020.

[2] Y. Chen, M. Li, P. Chen, and S. Xia, "Survey of cross-technology communication for iot heterogeneous devices," *IET Communications*, vol. 13, no. 12, pp. 1709–1720, 2019.

[3] J.-S. Shim, H.-J. Kim, N.-U. Lee, and S.-C. Park, "Design of zigbee-ble gateway direct communication system for smart home environment," in *Advances in Computer Science and Ubiquitous Computing*. Springer, 2017, pp. 1428–1433.

[4] E. Lee, Y.-D. Seo, S.-R. Oh, and Y.-G. Kim, "A survey on standards for interoperability and security in the internet of things," *IEEE Communications Surveys Tutorials*, vol. 23, no. 2, pp. 1020–1047, 2021.

[5] H. Hu, W. Song, Q. Wang, R. Q. Hu, and H. Zhu, "Energy efficiency and delay tradeoff in an mec-enabled mobile iot network," *IEEE Internet of Things Journal*, 2022.

[6] N. Bitar, S. Muhammad, and H. H. Refai, "Wireless technology identification using deep convolutional neural networks," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–6.

[7] V. Kumar, F. Li, F. Ye, and G. Subramanyam, “Autonomous wireless technology detection in seamless iot applications,” *IEEE Internet of Things Journal*, pp. 1–1, 2022.

[8] Y. Liu, H.-H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[9] Z. Deng, Q. Li, Q. Zhang, L. Yang, and J. Qin, “Beamforming design for physical layer security in a two-way cognitive radio iot network with swipt,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 786–10 798, 2019.

[10] W. Trappe, “The challenges facing physical layer security,” *IEEE communications magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[11] P. Gočal and D. Macko, “Eemip: Energy-efficient communication using timing channels and prioritization in zigbee,” *Sensors*, vol. 19, no. 10, p. 2246, 2019.

[12] V. Kumar, J. Yu, F. Ye, and G. Subramanyam, “A distributed approach to energy efficiency in seamless iot communications,” in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 1–6.

[13] V. Kumar, F. Li, J. Zhang, F. Ye, and G. Subramanyam, “A machine learning approach to modulation detection in wireless communications,” in *NAECON 2021 - IEEE National Aerospace and Electronics Conference*, 2021, pp. 341–347.

[14] T. J. O’shea and N. West, “Radio machine learning dataset generation with gnu radio,” in *Proceedings of the GNU Radio Conference*, vol. 1, no. 1, 2016.

[15] A. Garcia-Rodriguez, D. López-Pérez, L. Galati-Giordano, and G. Geraci, “Ieee 802.11be: Wi-fi 7 strikes back,” *IEEE Communications Magazine*, vol. 59, no. 4, pp. 102–108, 2021.

BIOGRAPHY

Venkataramani Kumar [Student Member, IEEE] (tiruchirappallinarv1@udayton.edu) received his Bachelor’s degree in Electronics and Communication Engineering from the SRM University, Chennai, India in 2017 with First Class and Distinction. He received his Master’s degree in Electrical Engineering from the University of Dayton, Ohio in 2019 and is currently pursuing his Ph.D. in Electrical Engineering at the same university. His research interests include the Internet of Things, wireless communications, and green communications.

Jiahui Yu [Student Member, IEEE] (yuj016@udayton.edu) is currently a Ph.D. student at the University of Dayton. He received his Bachelor’s degree in Nanjing University of Posts and Telecommunications, in 2017 and Master’s degree in Electrical Engineering from the University of Dayton, Ohio in 2019. His current research is on the Internet of things, wireless communications, and network security.

Fuhao Li [Student Member, IEEE] (lif003@udayton.edu) received the Ph.D. degree in the Department of Electrical and Computer at the University of Dayton, in 2022. He received a BS degree in Electrical Engineering from Dalian Jiaotong University, and an MS degree in

Electrical Engineering from the University of Dayton. His current research is in data mining, green communications, network security, network traffic classification with deep learning.

Jielun Zhang [Student Member, IEEE] (zhangj46@udayton.edu) is currently a Ph.D. candidate in the Department of Electrical and Computer at the University of Dayton. He received a BS degree in Electrical Engineering from Shanghai Normal University, a BS degree in Electronic and Computer Engineering Technology, and an MS degree in Electrical Engineering from Dayton. His research interests include Artificial Intelligence in networking, network security, network measurement, and the next-generation network.

Feng Ye [Senior Member, IEEE] (fye001@udayton.edu) received the BS degree from the Department of Electronics Engineering, Shanghai Jiaotong University, Shanghai, China, in 2011, and the PhD degree in Electrical & Computer Engineering from the University of Nebraska-Lincoln (UNL), NE, USA, in 2015. He is currently an associate professor in the Department of Electrical and Computer Engineering, University of Dayton, Dayton, OH, USA. His research interests include wireless communications and networks, artificial intelligence in networks, cyber security, and big data analytics. He is an associate editor of the IEEE Transactions on Vehicular Technology, IEEE Internet of Things Journal, and IEEE/CIC China Communications. He is a column editor of the IEEE Wireless Communications.

Sanjeevi Karri (sanjeevi@prixarc.com) received her Masters and PhD in Electrical Engineering from University at Buffalo, NY in 2004 and 2006, respectively. For the past 16 years she held various engineering and management positions working at leading semiconductor companies including Philips Semiconductors, NXP Semiconductors. She worked as Advisory Engineer at ASICNorth Inc before joining Prixarc LLC as Engineering Manager. At Prixarc, she has been serving as Principal Investigator in several SBIR projects sponsored by NGA, DTRA, DARPA, NASA, Navy and DOE. Her research interests include neuromorphic hardware, microelectronics, integrated circuits and sensors.

Guru Subramanyam [Senior Member, IEEE] (guru@prixarc.com) received his Bachelor's degree in Electrical and Electronics Engineering from the PSG College of Technology, (then affiliated with University of Madras) in 1984 with First Class and Distinction. He received his MS and

PhD degrees in Electrical Engineering with specialization in Microelectronics from the University of Cincinnati in 1988 and 1993 respectively. He is currently a Professor in the Department of Electrical and Computer Engineering, at the University of Dayton. His current research involves oxide thin films for electronics, electro-optics, energy and sensors. He is a senior member of IEEE. Professor Subramanyam won the 2008 Alumni Award for Scholarship at the University of Dayton, and 2007 IEEE Dayton section Harrell Noble Award for his achievements in electronic devices. In 2010, he was recognized by the Affiliate Societies Council as one of the outstanding engineers/scientists in the Dayton area in the category of research. In 2013, University of Dayton opened the Center of Excellence for Thin-film Research and Surface Engineering (CETRASE) under Professor Subramanyam's leadership. Professor Subramanyam co-founded Prixarc LLC in 2017 and currently serves as the Vice President.