Radio-in-the-Loop Simulation Modeling for Energy-Efficient and Cognitive IoT in Smart Cities: A Cross-Layer Optimization Case Study

Sebastian Boehm and Hartmut Koenig
ZITiS, Communications Department
Munich, Germany
eMail: {sebastian.boehm,hartmut.koenig}@zitis.bund.de

***Abstract*—Wireless communication technologies and Internet of Things (IoT) applications are the main drivers of upcoming sustainable Smart City networks which require an effective resource management. The reduction of the transmission energy consumption and the efficient utilization of the available spectrum for wireless communication, for instance, have to be enabled by energy-efficient and cognitive IoT networks. These are implemented through optimized communication protocol stacks and algorithms that rely on actual physical layer and channel state information. The modeling and the prototype evaluation of protocol optimization approaches are mainly driven by pure simulation studies with abstracted physical layer and channel models. With the Radio-in-the-Loop (RIL) simulation [1] and modeling [2], we have created an evaluation approach that integrates real wireless hardware and radio environments into the simulation of protocol sequences and algorithms. In this paper, we demonstrate a cross-layer optimization case study for energy efficient modeling using software-defined radios alongside this basic methodology. We exemplary show the scenario of a receiver-sensitivity control to increase the energy efficiency of receiver-dominated IoT nodes in Smart City networks.**

***Index Terms*—Hardware-in-the-loop, radio-in-the-loop, simulation, emulation, wireless sensor networks, cross-layer optimization, cognitive radio, cognitive iot**

I. Introduction

The Internet of Things (IoT) ecosystem of connected devices and sensors is growing rapidly. The next stage of expansion of smart devices and applications will be driven in spades by sustainable *Smart City* concepts. Comparable to wireless protocols for *Smart Home* applications, Smart City IoT technologies are also very diverse. Besides *cellular IoT* specifications (e.g., *LTE-M*, or *NB-IoT*), also wireless access technologies operating in license-free bands (e.g., *LoRaWAN*, or *Wi-Fi HaLow*) play a crucial role in Smart City automation concepts and applications. In case of Low Rate Wireless Personal Area Network (LR-WPAN), also *Bluetooth*, or Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 as basis for *ZigBee* or *Thread* are candidates of choice to implement wireless automation systems in the urban area. In particular, the environments in these new urban application areas are potentially very diverse. The transceivers must adapt to the dynamically changing conditions on the wireless radio channels. To this end, it is beneficial to consider cognitive radio decisions also at the higher protocol layers and applications related to wireless transmissions at the physical layer.

Simulation studies are usually the preferred preliminary step to analyze and evaluate new algorithms and protocol procedures. Accurate modeling of radio channel interactions and wireless transmissions are not feasible with reasonable computational effort here. Due to the nature of Discrete Event Simulation (DES), wireless link layer specification models usually do not include all the radio link features and services of the Medium Access Control (MAC) and Physical Layer (PHY) layers (e.g., Energy Detection (ED)). They usually omit specification details. For current research challenges in wireless transmission systems, however, these features need to be considered in detail. Therefore, we have to pose questions about how to achieve a modeling of radio interaction, complex physical phenomena and the coexistence with other wireless technologies within pure simulations.

The method of analog *radio channel emulation* in real hardware wireless testbeds is one of the last steps. It is mostly used for performance evaluation. This emulation technique allows one to setup reproducible wireless channel conditions for fully implemented smart devices, such as signal attenuation or noise and other signal sources (e.g., coexisting technologies). Considering the flexibility in analyzing and prototyping communication protocols, this methodology has crucial drawbacks because both access technologies and higher protocol layers with their implementations of the stacks poorly allow for customization and parameter studies.

In the following, Section II introduces the energy-efficient and *cognitive IoT* research area with its challenges in modeling and evaluation. With the methodology of the *Radio-in-the-Loop (RIL)* in Section III, we give an overview of the unique features of using real radio hardware in the *Split-Protocol-Stack* [1], [2] resulting from our parallel simulation and emulation experimentation in [3]. We state that this approach is designed to address current challenges in evaluating and prototyping both in terms of a specific wireless technology and as a general strategy for energy-efficient and cognitive IoT modeling. In this context, Section IV illustrates the modeling capabilities of the RIL simulation by means of a cross-layer optimization case study. The evaluation results demonstrate the achieved accuracy and modeling flexibility. In Section V, we give an outlook on further application areas and research trends in wireless Smart City communication networks.

II. Energy-Efficient and Cognitive IoT

One of the major optimization goals in resource-constrained wireless networks are energy-efficient wireless transmissions. These objectives are mainly solved in the domain of wireless access technologies via short on-air times (low duty cycle). Within the context of wireless communication, the term *cognitive IoT* refers to the cognitive capabilities of smart devices within their operating environment and connected network. For example, smart sensors make decisions about protocol parameters or spectrum and perform intelligent operation by analyzing network or radio conditions before transmitting. But all protocol layers and device parameters can be involved in the optimization of power consumption.

Cross-layer optimization is an essential concept for enabling cognitive capabilities. In contrast to modeling communications using reference designs (e.g., the Open Systems Interconnection (OSI) model), protocols and architectures can be optimized by violating layered communication based on performance, management, or security constraints. This results in new interfaces, redefinitions of layer boundaries, or a common coordination of parameters among the layers. However, implementing true node firmware for experimenting with cross-layer concepts is incredibly cumbersome. Network and protocol simulation are considered the state-of-the-art analysis and evaluation approach for cross-layer optimization due to its high flexibility in linking various modules and functions. In cognitive IoT networks also the higher protocol layers are effected by the spectrum management and need reconfiguration based on the PHY sensing information and the radio access scheduling (cp. [4] and [5] for the information exchange based on cross-layer interaction).

Cognitive radio refers to the ability of a transmitting and receiving device to make better use of the white spaces in the spectrum to counteract packet loss due to interference and noise. These concepts increase the robustness and resilience of the wireless networks and save transmission energy by reducing unnecessary retransmissions based on cognitive decisions. *Intelligent* and adaptive MAC procedures are also focused for optimizing the spectrum utilization in order to reduce packet collisions. Prototyping and evaluation of radio channel near optimization needs accurate Channel State Information (CSI). For example, the authors of [6] present a list of requirements for prototyping the MAC layer and highlight the need to have access to accurate PHY information to enable PHY reconfiguration. They conclude that mixed hardware-software architectures of embedded Software Defined Radio (SDR) platforms are the best choice to provide full flexibility and configurability.

In-network optimization refers to cognitive decisions of a scalable network. Protocol simulation offers very flexible possibilities to process state information of individual network nodes and communication links in abstract algorithms on middleware in the entire radio network. In the context of energy-efficient optimizations (e.g., network lifetime enhancement), issues of link quality, network utilization, data compression, transmission latency, jitter or Quality of Service (QoS) have to be considered here. Again, accurate information from the PHY and realistic feedback from the radio channel can significantly increase the validity of simulation-based evaluations.

In this highly relevant research areas, for example, a number of IEEE 802.15.4 [7] based optimization approaches are reflected only in the purely simulative evaluation. Besides MAC-based optimization originating from higher protocol layers (e.g., *adaptive access parameter tuning* in [8], or efficient network coordinator selection in [9] - both evaluated in pure DES), a number of approaches that require high accuracy and close interaction of the PHY should also be mentioned. The *transmission power control* approach in [10], evaluated in DES, is based on location information tables of mobile networks. It defines new service primitives for passing node range information to the PHY. In contrast, *receiver sensitivity control* in [11] is proposed to increase the energy efficiency of receiver-dominated nodes in IoT networks, evaluated based on pure virtual simulation in OMNeT++ [1] [12]. The radio propagation model is based on line-of-sight transmission, while no information is provided on modeling channel interaction over the PHY interfaces.

III. Radio-in-the-Loop Simulation Modeling

When considering practical contributions in the area of protocol stack-based network evaluation, Hardware-in-the-Loop (HIL) approaches emerge that differ in how hardware resources are represented in the overall design. These can be integrated by real components of a general purpose *host* computer system or correspond to real *external* devices. A further distinction can be made according to how protocol implementations of network devices are represented and what role simulation plays in the overall setup. This can be real hardware protocol implementations used in a *simulated network environment* or *simulated protocols* that interact with the network interface hardware. Related HIL approaches considering real protocol implementations in simulated networks (e.g., [13], [14]) are unsuitable for the analysis and further development of the above mentioned cognitive IoT research areas, as they offer insufficient flexibility in the modeling of protocol and application flows.

[1] OMNeT++ Discrete Event Simulator: https://www.omnetpp.org/

In contrast, the concept of integrating real wireless transmissions with simulated protocol stacks is still a largely untouched area of research. So far, related HIL approaches that couple network simulations with real hardware usually do not focus on accurate radio communication (e.g., integrating hardware prototypes in vehicular network communication simulation in [15].) Enabling real transmissions from the simulation is applied by Obermaier et al. [16] and Klingler et al. [17] who both present a single node device testbed for vehicular network HIL simulation based on IEEE 802.11p. They split the network architecture vertically to implement a virtual network bridge for transmitting link layer data frames via a single gateway node, called *physical twin* in [16], within an uncontrolled radio environment to the real device under test. Obermaier et al. discuss the difficult communication overhead and the inevitable real-time violations of a large number of *external events*.

A HIL wireless network evaluation with up to four nodes is introduced by Ding et al. [18], where configurable radio front ends and channel emulation techniques are used to control wireless transmissions. They do not include information on scalability and flexibility in modeling procedures within protocol stacks, and do not provide a variety of protocol models as is common in protocol simulation frameworks.

A. Radio-in-the-Loop Methodology

Based on our analysis, we argue that the functional requirements for accurate energy-efficient and cognitive IoT evaluation can be fulfilled by parallel simulation and emulation. With the methodology of *Radio-in-the-Loop (RIL)* a new strategy of evaluation is proposed, which allows parallel execution of protocol simulation and channel emulation. Testbed characteristics are achieved with emulated wireless transmissions and simultaneous simulated protocol flows and abstract algorithms on each sensor node. Thus, detailed channel state information can be obtained from an accurate emulated channel and PHY parameters can precisely be adjusted on real transceiver hardware or completely reconfigured based on SDR modules instead of applying abstract information for packet data in pure discrete event simulation.

In order to establish this novel methodology, some contributions have already been made by our work. Within the discrete-event protocol simulation, we achieve accurate representation of the MAC layer for an example reference wireless specification, the model of the IEEE 802.15.4 protocol standard in [19]. We have implemented DES extensions to transmit emulated events to RIL hardware nodes in [20] and practically investigated parallel simulation and emulation in [3]. In [2], we demonstrate details of the accurate modeling of the RIL interface according to the link layer protocol specification by exemplary focusing the IEEE 802.15.4 PHY. Meeting the challenge of synchronizing the simulation and the emulation domain for scalable network scenarios is introduced with the *Real-Time-Shift Simulation* approach for the superordinate *Split-Protocol-Stack* evaluation methodology in [1].

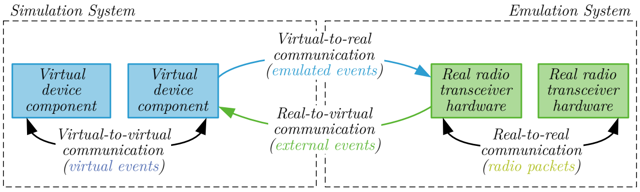
Simulation System
Emulation System
Virtual device component
Virtual device component
Real radio transceiver hardware
Real radio transceiver hardware
Virtual-to-real communication (emulated events)
Real-to-virtual communication (external events)
Virtual-to-virtual communication (virtual events)
Real-to-real communication (radio packets)

Fig. 1. Definition of terms and communication relations for the parallel simulation and emulation RIL methodology.

In Figure 1 the communication relations with terms and definitions for the RIL interfacing are presented. Representing the PHY from a *Split-Protocol-Stack*'s perspective is achieved by modeling the interfaces, protocol primitives, parameters, services, and internal procedures based on *virtual* components, *real* hardware and events. The RIL interface is responsible for exchanging *emulated* and *external* events between simulated nodes within the DES and real nodes on the testbed system. Furthermore, the *radio packets* represent real data transmission between real radio transceivers.

B. Radio-in-the-Loop Wireless Transmissions

The interface between the abstract modeling of protocols and algorithms in simulation and the provision of realistic environments on the radio channel is the *Radio-in-the-Loop (RIL)* approach. Essentially, this methodology creates the interfaces for simulation and emulation and represents the modeling of the PHY. Here all modeling areas of the radio interface are provided to interact with the real radio channel. The most important features to enable wireless packet transmission and reception are *modulation*, *carrier sensing*, *packet detection*, and *packet synchronization*. Usually a standard specification does not define how to implement or model these features on specific platforms. Furthermore, modeling of PHY functions for wireless transmissions in real hardware can conceptually be achieved in fundamentally different ways, e.g., either in software via the SDR concept or by implementing interfaces and firmware for real radio chip hardware.

With RIL wireless transmissions, we assume that real radio hardware (components) represent the radio transceiver interface of a communication system that is able to transmit and receive real radio packets. On the other hand, the hardware must be able to process several PHY functions, e.g., carrier sensing or ED (cp. PHY modeling responsibilities. Thus, the use of real transceiver hardware in wireless network simulations allows for an accurate representation of the PHY domains (e.g., symbol and waveform domains). Furthermore, the radio hardware takes over the interface function from the simulation domain to the real radio environment in the emulation domain.

The type of coupling can be accomplished either using a *gateway* architecture or a *one-to-one mapping* of bridged simulated and real nodes. While the former is primarily suitable to extend a real network by simulated nodes, the latter can achieve the increase in simulation accuracy aimed at in this work. From the simulators point of view, the emulation domain is considered as a *black box* and, on the other hand, the RIL gateway nodes only know the interface which generates the message input data. For each bridge node, a physical data communication interface to the control subsystem is necessary.

The *Chip-Radio-in-the-Loop* focuses on the use of standard-compliant radio chips of a given radio technology (e.g., IEEE 802.15.4). Implementing on a dedicated node firmware (cp. [3]) results in high accuracy with respect to the specification, but this method does not allow flexibility in extending and manipulating the PHY domains. The software radio-in-the-loop [2] approach provides the ability for the *Split-Protocol-Stack* to access emulated radio channels with the highest flexibility of PHY interfaces.

C. Software-Radio-in-the-Loop

The SDR-based RIL PHY implementation for the *Split-Protocol-Stack* was introduced in [2]. The example and reference model for the RIL transceiver is based on the *GNU Radio* framework[2], an open source, multi-threaded streaming system in which models are build from basic building blocks. In [2] the layered software radio transceiver processing flow based on the top-level SDR components is introduced in detail. We have modeled the transceiver according to the division of the link layer into MAC and PHY which can clearly be observed in the hierarchical module structure of our model. Accordingly, flexible experimentation ca be achieved including accurate PHY transceiver modeling. The Figure 2 exemplary shows the block diagram of the software-based modeling of a wireless packet data transmission. Likewise, other services of the PHY specification such as the ED or signal gain settings for receiving and transmitting are also implemented in software building blocks.

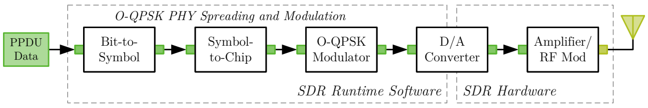

Fig. 2. Block diagram of an O-QPSK PHY SDR transmitter

IV. Case Study: Cross-Layer Optimization

The methodology of combining protocol simulation and radio channel emulation is suitable to meet the challenges in modeling and evaluation of future wireless networks and cognitive IoT. This approach has not yet established itself, but the potential of this technique is demonstrated in this case study for optimization at the receiver using RIL.

As mentioned above, optimization of performance parameters for transmitter and receiver is one of the main goals in cross-layer optimization regarding the PHY in energy-efficient IoT (e.g., increasing the energy efficiency with transmission power and receiver sensitivity control). The RIL methodology can be used to incorporate accurate real-world CSI for energy-efficient and reliable PHY transmissions in network simulations. Accordingly, we create here a use case and reference scenario that serves as an example of a *pure wireless* evaluation setup with no other simulated network nodes. It practically illustrates the contribution of parallel simulation and channel emulation for the evaluation of new approaches considering physical channel accuracy while maintaining protocol modeling flexibility. With this case study scenario, we demonstrate a receiver-dominated optimization based on the gain settings according to the radio packets signal strength measurement. In particular, it demonstrates the feasibility in a holistic *Split-Protocol-Stack* evaluation including SDR RIL transceivers. The overall goal of adjusting the receiver gain based on the Link Quality Indicator (LQI) and ED using SDR is similar to a *feedback control* and aims at minimizing the energy consumption of a receiver, which is definitely beneficial for maximizing the lifetime of sensor nodes in *Smart City* applications.

Whereas the ED is the most important part of the channel selection algorithm, the LQI indicates the reliability of a used wireless link. It is often a decision criterion for whether a partial channel or route is selected for transmission. For 802.15.4 transceiver hardware, it is not specified, how to use the LQI value, but it shall be performed for each received radio packet. Mostly it is implemented using a signal-to-noise ratio estimation and is represented as an integer ranging from 0 to 255 (lowest to highest quality). The result of the ED is also given in this range of values and represents the normalized received signal power (Received Signal Strength Indication (RSSI)).

The variations of the RSSI in reference measurements with deviations of several dB highlight the fact that environmental properties are hardly constant (cp. [21]). An efficient node placement with static configuration of the transmit power based on the signal strength measurements is therefore hardly feasible and wastes energy/battery capacity. Not least in the practical measurement studies, the potential for optimization became clear, as all packets are reliably received in a broader signal strength range. Looking at the results of our SDR RIL implementation in the following, with a bandwidth of approx. 20 dB difference in reception gain, all packets can be received without exception.

A. Energy Detection Measurement

A parameter study is required to determine favorable device parameters for general purpose SDR hardware and to

[2] GNU Radio is an open-source framework for development of SDR systems on general-purpose host systems: https://www.gnuradio.org/

estimate the possibilities of saving energy when transmitting and receiving packets. Exemplary, we performed several reference measurements with ordinary indoor channel characteristics in our office to evaluate the packet reception and parameter setting for the carrier sensing based on the ED signal probing with the specified normalization scheme. We set up a standard-compliant chip hardware (TI CC2420) placed at a distance of $0.75m$ from our software radio module to send a burst of 30 radio packets each. The Figure 3 shows the dependence of packet reception on the receiver interface gain setting (RX gain) based on the packet rate and signal strength.

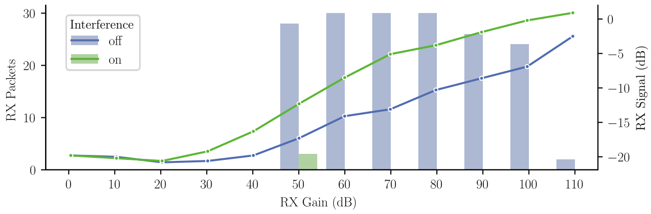

Fig. 3. Received signal strength and packet count at the software RIL model as a function of the receiver sensitivity (RX gain)

In the reception gain range of 60-80 dBm, all packets could be received by our software radio transceiver under realistic uncontrollable but largely interference-free environmental conditions. Moreover, a higher reception gain at the antenna has a clearly negative effect on the packet reception (ref. packet reception rate @ 110 dB in Figure 3). Thus, the receiver is already slightly overdriven due to the activated baseband amplifier. If the jammer is enabled (*Gaussian* noise with additional signal intensity around the transmit power) only a few packets are received at all due to the difficult or impossible decoding. Below 50 dB RX gain no packets could be received by the receiver because the signal-to-noise ratio for this environment is not sufficient. Based on such measurements, the threshold value for the ED can be determined or receiver-based optimization techniques can be explored.

B. Scenario Modeling and Definition

The abstract optimization goal for the cross-layer optimization scenario is to permanently keep the LQI for a communication link at 255 (maximum value) while minimizing the sensitivity at the receiver (RX gain). In existing 802.15.4 chip implementations, the receiver sensitivity cannot be adjusted at all or at least not uniformly according to a common guideline. Moreover, the standard does not define any protocol message and PHY parameters for setting the receiver gain but only minimum values. In the context of the RIL PHY, the modeling diversity of SDR transceivers is applied here. In a realistic channel emulation scenario, long-term measurements based on real transmissions can thus be evaluated without the need to develop real transceiver implementations for specific node hardware. An higher layer module in terms of an optimization algorithm in the simulation can be used to control this adjustments, but it requires access to the PHY and channel information. With only a few extensions, a simple information exchange across layer boundaries is enabled for parametrization of the RIL PHY transceiver hardware according to the *Split-Protocol-Stack*. Next, we explain these extensions to the simulation model.

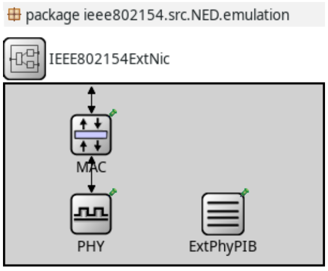

Fig. 4. The 802.15.4 OMNeT++ link layer module with external PHY PIB

1) PHY Information Database: IEEE 802.15.4 [7, Sec. 6.4, pp. 45f] defines PHY constants which are hardware dependent (cannot be changed during operation) and PIB attributes which are partially *read-only* parameters. As depicted in Figure 4, the PIB is provided in the simulation as a distributed database (simulation module) for all layers in this simplified cross-layer scenario. Therefore, new interfaces must be introduced in the involved protocol layers for communicating with this module (ref. ② in Figure 5). This approach and realization via an *external* database can be found in most cross-layer approaches in addition to direct individual cross-layer communication.

2) PHY Parameters: To enable a higher layer to perform adjustments of the RX gain based on the current LQI and ED values additional parameters must be introduced. The additional hardware parameters are provided by extending the PIB defined in the standard with additional information. They are transmitted via the original protocol primitives (`PLME-SET.request`'s and `PLME-GET.request`'s). Furthermore, the resulting external PIB cross-layer database is updated according to parameter-individual requests or for all attributes simultaneously according to a new protocol primitive `PLME-GET-PHY-PIB`. The manipulation of the database on the RIL hardware is restricted to the *external* PHY simulation module (ref. *emulated event* ⓐ between ② and ① in Figure 5), but higher layers can have access to the information and request to perform an attribute change (*virtual events* ⓑ).

For the exemplary receiver-dominated cross-layer approach, the following additional PIB attributes are defined.

- *phyLQI (link quality - from packet reception),*
- *phyEDvalue (channel energy - from signal),*
- *phyRXgain (sensitivity - according to amplifier gain).*

The application layer module (③ in Figure 5) is called `trafficgen` (adaptation of a standard OMNeT++ module

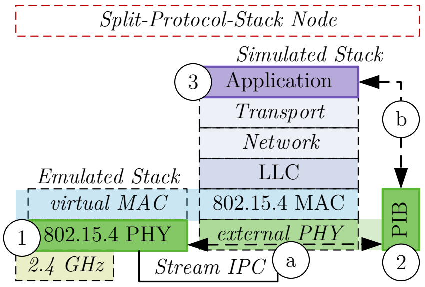

Fig. 5. Cross-layer PIB interaction from a higher layer of the protocol stack

for traffic generation). It implements a simple feedback control process according to the scenario definition and objective. The scenario is started in a configuration in which radio packets are received with maximum channel quality ($phyLQI = 255$). A feedback follows after each received packet via a gradual decrease of the receiver's sensitivity by adjusting the corresponding SDR hardware parameters as long as the channel quality does not change. Once the LQI deviates downward, the sensitivity is increased again to compensate this deviation.

C. Evaluation

Using our prototype implementation with OMNeT++ and *GNU Radio*, two measurement series with different radio channel settings were carried out as representative examples. A connection to the radio channel emulation could not be realized in this scenario, since the corresponding hardware interface connection for the SDR RIL concept is not yet realized within the prototype. As consequence, uncontrollable real conditions arise for an indoor radio channel, which are also suitable for this case study and demonstration. In the first experimental setup, the transmitter and receiver were placed at a distance of 1 m from each other and an initial RX gain of 90 dBm was configured to avoid noise due to the analyzed overload with too high receiver sensitivity in Figure 3. In the following you can see the RX gain optimization from LQI and ED as a function of the simulation time.

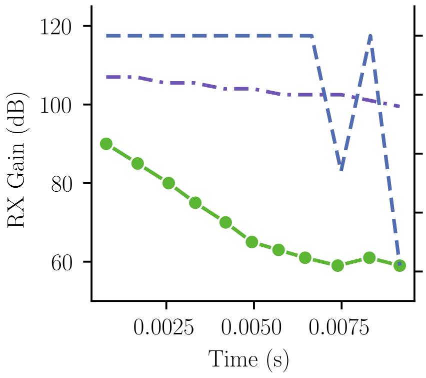

Fig. 6. LQI-based RX gain adaption (initialized with 90 dB)

The result in Figure 6 illustrates the potential of this type of receiver-dominated optimization. It shows the gradual reduction in gain at the receiver for each radio packet received over the simulated time. The RX gain at the antenna of the receiver can be reduced significantly (in the range of up to 30 dB) without degrading the channel quality and thus the fault tolerance for wireless data communication. Beyond a threshold of 59 dB, the channel quality LQI is no longer maximum under these conditions and is set back up one level by the feedback loop. Since the maximum value is again reached for the next radio packet, this process is now repeated continuously (depending on the conditions on the radio channel). Thus, this experimental setup demonstrates how to control a real-world wireless transmission based on an abstract algorithm within the network simulation.

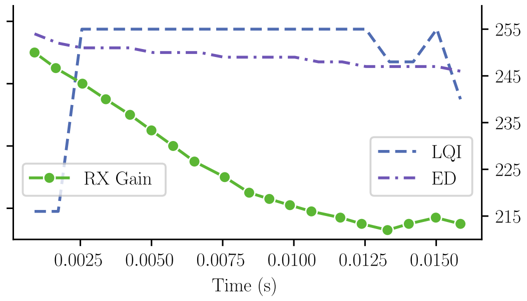

Fig. 7. LQI- and ED-based RX gain adaption (initialized with 110 dB, LQI below maximum)

The goal of the second experimental setup was to consider the largest possible link budget for the optimization. For this purpose, transmitter and receiver nodes were placed very close to each other (a few cm) and the measurement series were initially parametrized with a very high sensitivity of 110 dB gain at the receiver. Because of the high noise when dealing with high signal levels, the feedback algorithm additionally needs the signal energy ED to decide about reducing or increasing the RX gain (LQI below the maximum at high signal energy still leads to a reduction of RX gain). Thus, for each packet reception the LQI and ED values are evaluated for this exemplary demonstration. According to the results in Figure 7, the link quality in this setup is maximum within a link budget of 45 dB (100 dB to 55 dB) which allows for significant energy consumption optimization on the receiver. The implementation of the event handling in the OMNeT++ module `trafficgen` is presented in the following.

In the same way, the transmitter can be parametrized to reduce the transmission energy in a control loop based on the evaluation of the received *acknowledgments*. A corresponding attribute for the hardware configuration of the transmission power (*phyTXgain*) is also part of our extensions for the external PIB. Of course beyond this simple scenario, other criteria and parameters can be included in the optimization.

V. Conclusion and Outlook

With this case study evaluation, we exemplary present a first scenario of the *Radio-in-the-Loop (RIL)* simulation for the model-based prototyping and evaluation, where parameters can be easily changed within the algorithmic simulation and SDR domain. Thus, algorithms do not need to be implemented in protocol stacks and firmware. The achieved results demonstrate the feasibility of the approach for modeling a cross-layer optimization strategy with the parallel simulation and emulation. For practical use, it shows the possibility to ensure reliable transmissions while reducing the gain in reception at the same time. Furthermore, the energy consumption of the RIL hardware modules can be recorded simultaneously for analyzing the energy-efficiency. Some more practical and theoretical considerations or concrete extensions of the scenario may cover different state-of-the-art research areas.

The battery life of wireless devices is certainly reduced by *radio spectrum pollution*, as the nodes have to transmit above the noise level which in turn creates additional interferences. As digital transformation continues, radio usage of areas and hotspots is increasing rapidly due to various technologies. The current and upcoming IoT and *Smart City* concepts with countless surrounding wireless devices within the urban area will make this situation much worse. Dense radio conditions are neither easy to determine nor predict, and even more difficult to model for *radio network planning*. The purely simulative modeling of radio interference and pollution causes an incredible effort and therefore often remains abstract or a theoretical consideration. However, taking these effects into account will become increasingly important in the prototyping and performance evaluation of modern techniques and optimization methods due to the expanding penetration of wireless technologies in the future. In our simplified case study optimization approach, we have already been able to demonstrate, how an evaluation of intelligent approaches can be achieved by including real or emulated radio environments by means of *RIL*. Future research activities in wireless communication modeling will inevitably depend on the simulation of algorithmic flows with real-world accuracy or emulation capabilities.

Cross-layer optimization and *cognitive radio* have been a continuously growing, red-hot research focus for more than a decade now. Current activities on cognitive radio networks address, for example, research issues of *energy harvesting* for *spectrum-efficient networking* in the IoT [22] jointly consider radio transceiver design and network data transmissions. Concrete evaluation results are mostly determined pure simulatively. Regarding *security vulnerabilities* in untrustworthy urban environments, the radio packet parameters can be evaluated in detail. If a packet is received with a deviating radio fingerprint (e.g., signal strength, or *time difference of arrival*), an intelligent higher layer algorithm can trigger an alarm or interrupt the communication. PHY- and channel-accurate model-based evaluation and prototyping of such approaches can be extended with real-world measurements from RIL SDRs. Further cross-layer consideration of parameters from several protocol layers is also conceivable, so that an intelligent algorithm considers both simulatively generated parameters and real hardware attributes from different node and network properties.

Deep Learning for future wireless communications is an emerging interdisciplinary paradigm which will revolutionize wireless networking by means of artificial intelligence. For example, these strategies evaluate several hardware parameters and CSI for a period of time to decide which physical parameters should be configured for a transmission. Recent studies, surveys, and approaches (e.g., [23]–[25]) show how *Deep Learning* on the physical layer and radio channel can stimulate transmission algorithms or transceiver design for coexistence of multiple radio access technologies or optimal transmission links for ultra-low latency constraints in dense networks. Specific solutions concern, for example, the channel coding in [26] or the modulation classification based on *Neural Networks* in [24]. Therefore, *radio fingerprinting* and *spectrum analysis* for feature engineering in *Neural Networks* are key elements. We consider our SDR RIL methodology for acquiring features of the radio channel to enable prototyping for reconfigurable PHY using software building blocks an important step in this direction. Holistic modeling using the RIL concept is perfectly suited for parameter studies from real-world measurements in the simulation. Existing machine learning algorithms can easily be integrated into DES in a higher programming language (e.g., *C++* or *Python*).

In future work, the RIL SDR modules need to be fully integrated within the analog radio channel emulation platform to enable scalable experiments with multiple nodes. In this context, minimizing the scheduling jitter of the event execution when using general-purpose SDR devices should be an important goal to reliably achieve maximum accuracy on the RIL hardware (cp. scheduling jitter in [2]). Furthermore, the synchronization [1] must be expanded to the controllers on the radio channel emulation hardware.

According to the framework modeling philosophy (e.g., OMNeT++ / INET *modules*, or GNU Radio *blocks*), the RIL simulation capabilities can be provided for various standards, protocols, or further wireless link layer technologies for which there is often already support for the used environments. In order to enable broad support for current wireless technologies within the context of *Smart Cities*, the next steps will be to integrate the latest specifications as models for the DES and SDR streaming systems. Therefore, existing models for *cellular IoT*, or *LoRaWAN* (e.g., [27], or [28]) must be examined for accuracy and conformance to specifications. Implementation of the appropriate shared protocol libraries and generation of *external* and *emulated* events for transmission and handling of protocol messages are the steps to support the intended wireless technologies for RIL.

References

[1] S. Böhm and H. König, “Real-time-shift: Pseudo-real-time event scheduling for the split-protocol-stack radio-in-the-loop emulation,” in *Proceedings of the 25th International Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWiM)*. ACM, 2022.

[2] ——, “Split-protocol-stack wireless network emulation: Enabling phy modeling diversity with software-radio-in-the-loop,” in *Proceedings of the 17th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet '21)*. ACM Press, 2021, p. 8.

[3] ——, “Semulate: Seamless network protocol simulation and radio channel emulation for wireless sensor networks,” in *Proceedings of the 15th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*. IEEE, 2019, p. 8.

[4] S. Pandit and G. Singh, “Framework for cross-layer optimization in cognitive radio network,” in *Spectrum Sharing in Cognitive Radio Networks*. Springer International Publishing, 2017, pp. 225–251.

[5] A. B. Ozgur, O. Karli, and O. Ergul, “Cognitive radio sensor networks,” *Network, IEEE*, vol. 23, no. 4, pp. 34–40, 2009.

[6] F. V. Gallego, J. Alonso-Zarate, C. Verikoukis, and L. Alonso, “A survey on prototyping platforms for the development and experimental evaluation of medium access control protocols,” vol. 19, no. 1, pp. 74–81.

[7] IEEE Standards Association, “Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs),” 09 2006.

[8] M. D. Francesco, G. Anastasi, M. Conti, S. K. Das, and V. Neri, “Reliability and energy-efficiency in IEEE 802.15.4/ZigBee sensor networks: An adaptive and cross-layer approach,” vol. 29, no. 8, pp. 1508–1524.

[9] F. Cuomo, A. Abbagnale, and E. Cipollone, “Cross-layer network formation for energy-efficient IEEE 802.15.4/ZigBee wireless sensor networks,” vol. 11, no. 2, pp. 672–686.

[10] M. Al-Jemeli and F. A. Hussin, “An energy efficient cross-layer network operation model for IEEE 802.15.4-based mobile wireless sensor networks,” vol. 15, no. 2, pp. 684–692.

[11] P. Detterer, M. Nabi, H. Jiao, and T. Basten, “Receiver-sensitivity control for energy-efficient IoT networks,” vol. 25, no. 4, pp. 1383–1386.

[12] A. Virdis and M. Kirsche, Eds., *Recent Advances in Network Simulation*. Springer International Publishing, 2019.

[13] E. Weingärtner, H. vom Lehn, and K. Wehrle, “Device driver-enabled wireless network emulation,” in *Proceedings of the 4th International Conference on Simulation Tools and Techniques (SimuTools)*. Barcelona, Spanien: ICST, 3 2011.

[14] S. Unterschütz and V. Turau, “A hybrid testbed for a seamless combination of wireless sensor networks and omnet++ simulations,” in *11. GI/ITG KuVS Fachgespräch Sensornetzwerke*. Darmstadt, Deutschland: GI/ITG, 9 2012, pp. 52–55. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.348.6422

[15] D. S. Buse, M. Schettler, N. Kothe, P. Reinold, C. Sommer, and F. Dressler, “Bridging worlds: Integrating hardware-in-the-loop testing with large-scale VANET simulation,” in *2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*. IEEE, feb 2018.

[16] C. Obermaier, R. Riebl, and C. Facchi, “Fully reactive hardware-in-the-loop simulation for VANET devices,” in *Proceedings of the 21st International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2018.

[17] F. Klingler, G. S. Pannu, C. Sommer, and F. Dressler, “Poster: Connecting simulation and real world: Ieee 802.11p in the loop,” in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (MobiCom)*. ACM.

[18] L. Ding, Y. Sagduyu, J. Yackoski, B. Azimi-Sadjadi, J. Li, R. Levy, and T. Melodia, “High fidelity wireless network evaluation for heterogeneous cognitive radio and networks,” in *Proceedings of the SPIE Defense, Security, and Sensing Conference*, 5 2012.

[19] M. Kirsche and M. Schnurbusch, “A new ieee 802.15.4 simulation model for omnet++ / inet,” in *Proceedings of the 1st International OMNeT++ Community Summit (OMNeT)*, 09 2014. [Online]. Available: http://arxiv.org/abs/1409.1177

[20] S. Böhm and M. Kirsche, “Unifying radio-in-the-loop channel emulation and network protocol simulation to improve wireless sensor network evaluation,” in *Simulation Science*, M. Baum, G. Brenner, J. Grabowski, T. Hanschke, S. Hartmann, and A. Schöbel, Eds. Springer International Publishing, 2018, pp. 219–238.

[21] M. S. Hossen, M. K. B. Kamal, and M. S. Rahman, “Consistency analysis of RSSI measurement for distance estimation of wireless sensor nodes,” in *Proceedings of the 15th International Conference on Computer and Information Technology (ICCIT)*. IEEE, dec 2012.

[22] J. Ren, J. Hu, D. Zhang, H. Guo, Y. Zhang, and X. Shen, “RF energy harvesting and transfer in cognitive radio sensor networks: Opportunities and challenges,” vol. 56, no. 1, pp. 104–110.

[23] Z. Qin, H. Ye, G. Y. Li, and B.-H. F. Juang, “Deep learning in physical layer communications,” vol. 26, no. 2, pp. 93–99, 2019.

[24] T. O'Shea and J. Hoydis, “An introduction to deep learning for the physical layer,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 563–575, dec 2017.

[25] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, and M. Cao, “Deep-learning-based physical layer authentication for industrial wireless sensor networks,” *sensors*, vol. 19, no. 11, p. 2440, 2019.

[26] H. Kim, S. Oh, and P. Viswanath, “Physical layer communication via deep learning,” vol. 1, no. 1, pp. 5–18.

[27] M. Slabicki, G. Premsankar, and M. D. Francesco, “Adaptive configuration of lora networks for dense IoT deployments,” in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, apr 2018.

[28] J. Tapparel, O. Afisiadis, P. Mayoraz, A. Balatsoukas-Stimming, and A. Burg, “An open-source LoRa physical layer prototype on GNU radio,” in *Proceedingsof the 21st IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE.