Impairment Shift Keying: Covert Signaling by Deep Learning of Controlled Radio Imperfections

Kunal Sankhe, Francesco Restuccia, Salvatore D’Oro, Tong Jian, Zifeng Wang, Amani Al-Shawabka,
Jennifer Dy, Tommaso Melodia, Stratis Ioannidis, and Kaushik Chowdhury
Northeastern University, Boston, MA, USA

Abstract—**The broadcast nature of the wireless spectrum necessarily implies the possibility of eavesdropping, as well as malicious modification of waveforms through inexpensive, widely available software-defined radios (SDRs). This paper proposes a method for covert wireless communications that can be used to authenticate a device or exchange private information between devices. Our approach, called *Impairment Shift Keying* (ISK), introduces small yet controlled modifications to the radio transmitter hardware, which distorts regular standards-compliant waveforms, such as WiFi, with only 1% increase in bit error rate. A deep convolutional neural network (CNN) is trained to learn these overlay signal variations, which serves as a low-overhead classifier returning a binary 0 or 1 per detected impairment pattern. By mapping device-specific injected impairment patterns to signal variations, ISK validates device IDs with only few inphase (I) and quadrature (Q) samples. Furthermore, through an experimental testbed, ISK is shown to be resilient to channel and SNR level variations, allowing a throughput of 93-1500 Kbps on the covert channel that is undetected by other receivers.**

I. Introduction

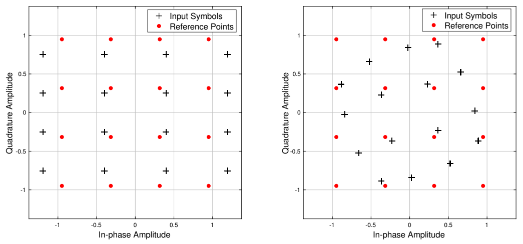
The broadcast nature of wireless channel makes communication vulnerable to eavesdropping, message modification or device impersonation. Given recent instances of malicious actions [1], we aim to add an overlay layer that can transfer confidential information, and also ensure robustness to software-based ID-spoofing. In classical network architecture, information is encrypted using cryptographic techniques. However, with this approach, the devices themselves must be capable of performing computationally involved operations, which may impact deployment in low-cost sensors [2], [3]. Secondly, even if information cannot be decoded, the device MAC ID can be forged to impersonate a different device. These observations motivate our desire for realizing a new paradigm of *completely covert communication*, with many potential applications in the space of consumer IoT and military operations.

• **Limitations of existing approaches**: Some prior work on covert channel design leverages prior knowledge of the underlying wireless standard. For example, [4] embeds information in the unused padding bits in the physical layer data units of WiFi frames. Other works create covert channels by encoding information on top of unused subcarriers [5], [6], the training sequences of WiFi [7], and the cyclic prefix of WiFi OFDM symbols [8]. The authors in [9] create side channel by changing the spatial position of almost blank subframes within a standard LTE frame, whereas a concurrent data and energy transmission is proposed in [10]. The main challenge in these approaches are that they are tailored to specific protocols (*i.e.*, WiFi, Bluetooth), and thus not generalizable for new/emerging standards. Moreover, all of them require modifications to the protocol with additional transmitter-side signal processing.

When specific modulation schemes for the transmitted waveform are known a priori, the constellation diagram can be distorted in a controlled manner. In [11], the authors hide symbols by replacing existing constellation points with additional “dirty” constellation points. A pseudo-noise asymmetric shift keying (PN-ASK) modulation scheme is proposed in [12], where overlay symbols are added to an existing waveform by shifting the original symbol amplitudes. In [13], authors encode covert information by introducing an additional fading-like effect using a filter at the transmitter. While the above works are not dependent on a specific standard, they do require pre-decided in-phase/quadrature (IQ) constellation features (such as, the modulation *must be m-PSK*). These methods are also dependent on channel conditions as amplitude changes within constellation points cannot be reliably predicted or replicated in future unseen channel conditions.

To address the limitations of existing work, this paper proposes a novel technique of embedding a covert side-channel in a regular signal transmission in a method called *impairment shift keying* (ISK). The core concept of ISK is simple yet effective: it injects a series of so called *impairments* at the transmitter’s side, such as DC offset and IQ imbalance, which in turn introduces controlled changes in the resulting transmitted signal constellation. Note that ISK can work for *any* protocol supporting m-PSK or m-QAM based modulation scheme, giving greater flexibility over [12]. Our approach ensures that general receivers that hear the modified signal do not observe any discernible increase in the BER owing to the constellation distortion. Additionally, while our approach is agnostic of the wireless standard, we demonstrate results on 802.11a WiFi links in an experimental testbed.

• **ISK approach**: ISK leverages tiny process imperfections within mass-produced transceivers. Wireless circuits present within the analog components (*e.g.*, digital-to-analog converters, band-pass filters, frequency mixers and power amplifiers) that compose a typical transmission chain have different tolerances and exhibit age-related performance degradations that compose a unique *signature* of a device. Fig. 1 indicates an example scenario of two impairments, namely IQ imbalance and non-linear distortion of the amplifier for a 16-QAM constellation. The red circles indicate the ideal constellation points formed by the I (x-axis) and Q (y-axis) components of a given sample, and the black crosses indicate actual constellation



(a)

(b)

Figure 1: Effect of RF impairments a) IQ Imbalance b) Amplifier Non-linear Distortion on 16-QAM modulated symbols.

points that are shifted. These shifts form a unique signature and have been exploited as fingerprints for radio identification [14]. ISK takes this one step forward: it leverages them to secretly embed covert information within WiFi frames by first minimizing the device imperfections through calibration and then intentionally re-introducing the artificial impairments on the transmitter through USRP Hardware Driver (UHD) software API commands. At a high level, these impairments introduce similar effects as a fading channel. Standard receivers and wireless standards are designed to cope up with such variations in the signal, and hence their performance does not significantly decrease when additional information is embedded through impairments.

In ISK, the receiver first determines a set of feasible impairments, such that when they are introduced at the transmitter side, the BER observed by a regular (here, WiFi) receiver is not impacted. The transmitter then selects pairwise impairments $\{I_k, I_l\}$ as a feasible set and then maps a binary covert data to the chosen impairment tuple as: $\{0 \rightarrow I_k, 1 \rightarrow I_l\}$. These imbalances and offsets are then intentionally introduced at the transmitter. In order to thwart spoofing attacks from an adversary that may learn these impairments, the receiver changes the pairwise impairments after every successful packet transmission.

• **Using ISK with deep learning for covert channel:** Deep learning techniques have shown great promise in image and speech identification problems, and are steadily gaining traction in applications within the wireless domain [15]. As such, ISK leverages a convolutional neural network (CNN) architecture for device fingerprinting [14], [16]. Other works have used different deep CNN for modulation [17] and protocol identification [18]. We train the CNN *a priori* to detect the choice of the impairment made at the transmitter side from the received IQ samples alone, even when every other parameter is the same, including the same MAC ID. ISK requires the receiver to predict a sequence of impairments –introduced intentionally– at the transmitter, which provides the basis of the covert channel.

We summarize the main contributions of this paper:

• First, we study the different causes of transmitter-side signatures, and visualize their impact on the IQ constellation space. We identify specific features that are amenable to fine tuning by the receiver feedback using software APIs.

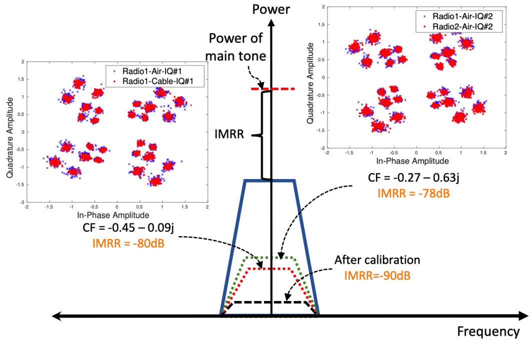


Figure 2: Image signal to quantify IQ imbalance through IMRR and its effect on demodulated data for 2 IMRR values on 2 radios under 2 channel conditions.

• Then, we identify the feasible set of impairments that are then trained using a CNN. This is a critical step towards a 'train once deploy anywhere' paradigm that allows robust learning and accurate prediction under realistic channel variations, near-perfect accuracy.

• Finally, we implement ISK on USRP X310 radios. Experimental results reveal that ISK achieves a throughput of 93 Kbps at 15dB SNR level, which can be improved up to 1500 Kbps under specific SNR conditions.

II. Selection and Learning of Feasible Impairments

In this section, we discuss the role of impairments in generating unique pattern in demodulated data, and show that the impairments (i) are independent of the environment, and (ii) do not apply only in context of a specific transmitter-receiver pair (as opposed to, say, relative phase offset). In ISK, training process is designed so that the CNN can classify the unique patterns generated by these controlled impairments, *irrespective of the radio that incorporates them.*

A. SDRs and selection of feasible impairments

We first explain the use of self-calibration utilities provided by National Instruments (the manufacturer of the SDRs used in this paper) to introduce controlled impairments. We focus only on IQ imbalance owing to space constraints, though our approach can be trivially extended for combination of other impairments, such as DC offset. IQ imbalance causes interference in the signal by generating its image at a mirror frequency. It is quantified by measuring the power of the image with respect to the desired signal, also called as Image Rejection Ratio (IMRR), as shown in Fig. 2.

While many theoretical time and frequency domain methods allow compensation for the IQ imbalance, we use the Ettus-provided UHD calibration utility `uhd_cal_tx_iq_balance`. At runtime, the UHD software automatically applies the correction, typically a single complex factor, to the transmit chain of the RF daughterboard. We modify the calibration utility to record the correction factor (CF) and corresponding IMRR.

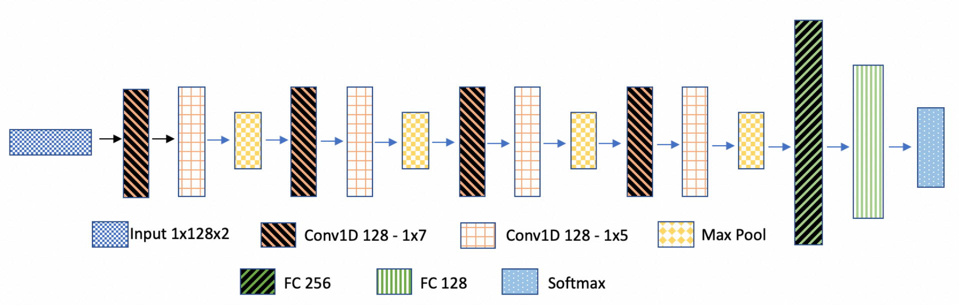


Figure 3: Our proposed CNN architecture with 8 convolution 1D and 2 fully connected layers.

ISK intentionally introduces IQ imbalance for the desired IMRR in the transmitter SDR by selecting the corresponding CF from a pre-recorded table and applies them using the `set_iq_balance` GNU radio function. The level of intentional introduction of IQ imbalance is controlled so that the signal acquires unique characteristics that are robust to channel- and device-variations. To demonstrate this, consider the demodulated signals captured from two USRP X310 SDRs over air and cable in Fig. 2. The left plot shows a unique pattern of demodulated data, when ISK sets IQ imbalance with IMRR of -80dB by selecting CF of $-0.45-0.09j$ in the same transmitter radio for two channels, *i.e.*, cable and air. The right plot shows demodulated data obtained when ISK introduces IQ imbalance of IMRR -78dB using CF $-0.27-0.63j$ for two different radios under the same channel conditions. Thus, we note that adding the same level of IQ imbalance results in virtually the same pattern in each case, ensuring repeatability and robustness under channel- and device-variations.

Among many IMRR values of IQ imbalance, ISK automatically selects feasible impairment values that produce IQ sample constellation points that are significantly different from each other, while minimizing the influence on the BER for the transmitter. This step allows ISK to pre-train on impairment patterns, which are shown in Fig. 2 to be both device and channel agnostic. We refer the steps proposed in Sec. V-B of our earlier work [14] to identify feasible set of impairments.

B. CNN classifier using transmitter-side impairments

ISK uses a deep Convolutional Neural Network (CNN) to identify an unique pattern of demodulated IQ symbols. We use one-dimensional (1D) convolutions to capture the local temporal relations within IQ symbols, which carry subtle identifying information of impairments. Since we rely on only those hardware impairments that do not vary over time, their effect on the transmitted signal can be identified in different local portions of the entire received waveforms. Indeed, 1D CNNs are particularly effective at these kind of tasks, *i.e.*, identifying features from fixed-length segments of the complete dataset when the location of such features within the segment are not highly correlated. ISK operates 1D convolutions along the time axis and uses I and Q data as two distinct channels of the 1D sequence.

The main building block of the proposed CNN model consists of two 1D-convolution layers, each with 128 filters of size 7 for the first layer and 5 for the second one. These two convolutional layers are followed by a Max Pooling layer, used to provide (a) shift invariance and (b) reduce the dimensionality of the output feature maps of the preceding convolution layer, while retaining the most important information. We then stack 4 of such building blocks, followed by a set of 2 Fully Connected (FC) layers, composed of 256 and 128 neurons respectively, and a Softmax classifier layer. In order to overcome overfitting, we set the dropout rate to 50% at the FC layers. For training, we choose a sliding window approach to partition the input signals into overlapping sequence of samples, referred as slices. This enhances the shift invariance of the features learned by the CNN. Note that all IQ samples for training are collected over the cable, *i.e.*, we remove the influence of wireless channel so that the CNN can learn the pattern generated solely by hardware impairments.

ISK deliberately introduces random noise by modifying the original data to augment the initial dataset before it is given as input to the classifier. Since low SNR of the received samples results in scattering around the ideal constellation point location within the IQ plane, the noise is modeled as a Gaussian variable.

III. Design of Covert Channel

The ISK scheme (i) encodes covert information by mapping binary data to pairwise impairments that are intentionally injected in the WiFi transmitter; (ii) authenticates the transmitter by matching stored and received copies of a random binary pseudo-noise identification key; and (iii) prevents ID-spoofing by changing the identification key and pairwise impairments after every successful packet transmission.

A. ISK's phase-wise operation

First, we discuss an overview of ISK organized into three successive phases.

Phase-1: Authentication via a random PN binary sequence: An authorized transmitter-receiver pair uses a linear-feedback shift register (LFSR) to produce a sequence of pseudo-random binary numbers known at both sides of the link. This can be achieved by exchanging a starting seed for the LFSR prior to deployment in the field, so that the transmitter and receiver operate in a lock-step fashion. Alternately, in real-time, the receiver can share the coefficients of the LFSR through a secure channel. Thus, the receiver uses this sequence as an '*identification key*' to authenticate the transmitter. Consider

Table I: Pairwise Impairments

Index	$0 \rightarrow I_k$	$0 \rightarrow I_l$
0	I_1	I_4
1	I_4	I_3
$\vdots$	$\vdots$	$\vdots$
7	I_2	I_1

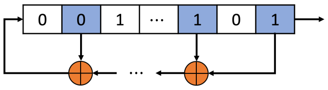


Figure 4: Linear Feedback Shift Register (LFSR)

'0011110' as the LFSR output sequence that will be used for the rest of this discussion.

Phase-2: Covert data transmission through Impairment Shift Keying (ISK): The set of feasible impairments $\mathbf{I} = \{I_1, I_2, \ldots, I_K\}$ is chosen so that any element of this set, when applied at the transmitter side, does not degrade the BER of the transmitted waveform beyond a pre-set threshold. The measured SNR at the receiver plays a critical role in selecting this set, and hence, is created at the receiver side. The receiver first determines the upper bound on the impairment level, say I_S by measuring the SNR for a given transmitter that just satisfies the BER constraint. After determining I_S, the receiver first randomizes the ordered set of allowed impairments, $[I_1, I_2, ..., I_S]$, where $BER_{I_1} < BER_{I_2} < \cdots < BER_{I_S}$, and then chooses pairwise permutations from this set.

Thus, it creates a subset of tuples $\{I_k, I_l\}$ from the set of all possible impairments, wherein there is a direct mapping of the binary representation as follows: $\{0 \rightarrow I_k, 1 \rightarrow I_l\}$. This mapping is sent to the transmitter and then utilized at the latter to alter the transmitted waveform of each bit, by modifying the symbol constellation through the chosen impairment. This intentional 'distortion' of the symbol constellation may appear as an arbitrary channel effect to a potential eavesdropper, though it is anticipated at the authorized receiver, as it shares the same mapping table with the transmitter. After every successful packet transmission, the transmitter and receiver change the pair of impairments in a synchronized fashion to further ensure secrecy and resilience to playback attacks.

For example, assume that the transmitter supports a maximum impairment level up to I_4. The receiver first randomizes the ordered set $[I_1, I_2, I_3, I_4]$ and finds the $2^V = 8$ permutation pairs listed in Table I, where $V = \lfloor \log_2(^4P_2) \rfloor = 3$. Out of total permutations of $^SP_2$, the receiver selects the first 2^V permutations, where $V = \lfloor \log_2(^SP_2) \rfloor$ to generate a table. Each row in the table is a pair of impairments $\{I_k, I_l\}$ to be used to represent a binary 0 and 1, respectively, and this selection is constant for the entire ISK packet transmission.

Note that each transmitter can have a different table due to different upper bounds on impairment level I_S, and due to randomized permutations giving the pairwise impairments. This further enhances the security of our covert communication, while guaranteeing the BER constraint for the regular WiFi transmitter radio.

Each ISK encoded packet has three fields: '`Preamble`', '`ID`' and '`Covert Data`'. ISK uses a fixed-length binary '`Preamble`' sequence for synchronization, whereas the 'identification key' obtained in Phase-1 is used as '`ID`'. The receiver uses '`ID`' to identify and authenticate the sender of the packet. '`Covert Data`' is the last field in the packet and carries a secret information intended for the target receiver. For each binary value 0 or 1 in the ISK packet, the transmitter maps the impairments as: $\{0 \rightarrow I_k, 1 \rightarrow I_l\}$ for a fixed number of baseband symbols. '`Preamble`' is always conveyed with a pair of fixed impairments $\{I_1, I_2\}$, where $BER_{I_1}, BER_{I_2} < BER_{I_j}$ for $j > 2$.

After every successful packet transmission, the transmitter selects the first V bits of '`ID`', which is the binary sequence output of the PN generator towards selecting the next pair of impairments. For e.g., for the ID '0011110', the transmitter selects $\{I_4, I_3\}$ as the next pair of impairments from Table I based on the first $V = 3$ bits of '`ID`'. The receiver also chooses the same pair of impairments to decode the packet.

Phase 3: ISK packet decoding at the target receiver: The receiver uses ISK's trained CNN classifier described in Sec. II-B to determine the sequence of impairments used by the transmitter. A CNN classifier uses an input slice of demodulated symbols to get the prediction probabilities over all feasible impairments. Since the receiver knows the pair of impairments used by each transmitter radio, it uses prediction probabilities of those specific impairments $\{I_k, I_l\}$. The receiver first synchronizes with impairment pair $\{I_1, I_2\}$. It later uses $\{I_k, I_l\}$ to decode '`ID`' and '`Covert Data`'. For authentication, the receiver extracts the binary sequence within '`ID`' and matches with the binary sequence output from its own PN generator specific to that particular transmitter radio. After successful identification, the receiver decodes the covert message in the same way.

After successful identification and data decoding (communicated implicitly through a regular link layer ACK), both the transmitter and receiver generate a new binary sequence to create a different identification key. This in turn changes the pair of impairments that will distort the transmitter-signals, as described in Phase 2. ISK allows the impairment-based fingerprinting to scale to thousands of radios requiring a minimum of just two impairments. Additionally, switching the identification key and the pair of impairments on a per-packet basis makes it hard for the adversary to learn the pattern and perform spoofing attack. Thus, we claim ISK based covert communication is *scalable* as well as *secure*.

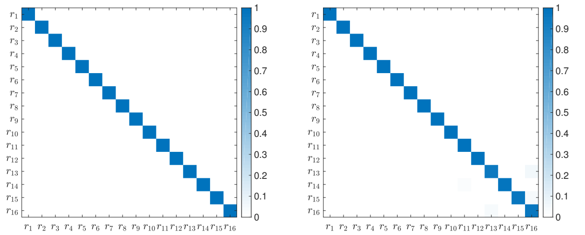
B. ISK throughput analysis

This section studies the throughput of ISK's covert channel, defined as the number of bits correctly decoded per unit time. First, we provide calculation of maximum throughput for IEEE OFDM based 802.11 a/g/n/ac standards.

Consider N as the FFT size of an OFDM system and N_d is the number of subcarriers used for data communication. In IEEE 802.11 a/g/n/ac, $N = 64$, whereas $N_d = 48$ in 802.11 a/g and $N_d = 52$ in 802.11 n/ac. Each data subcarrier is independently modulated with M-QAM or M-PSK modulation scheme. If the receiver sampling rate is R_s Msps, the useful symbol duration is $t_u = \frac{N}{R_s}$. If t_g is the Guard Interval (GI), then single ODFM symbol duration is $t = t_u + t_g$. Since ISK

Slice Size	T_{max} in Kbps 802.11a/g	T_{max} in Kbps 802.11n/ac
128	93.75	101.56
64	187.5	203.12
32	375	406.25
16	750	812.5
8	1500	1625

Table II: Maximum throughput of ISK's covert channel for different slice size



(a) (b)

Figure 5: Classification accuracy (a) over air in-indoor environment; (b) over air in open recreation area

modulates each binary data in n_{slice} baseband data symbols, ISK's maximum throughput is $T_{max} = \frac{N_d}{t \times n_{slice}}$ bps.

To illustrate this, consider 802.11a WiFi OFDM system with $N = 64$, $N_d = 48$, $R_s = 20$ Msps. Therefore, useful symbol duration $t_u = \frac{20 \times 10^6}{64} = 3.2\mu$s. Assuming GI interval $t_g = 0.8\mu$s, then OFDM symbol duration is $t = 4\mu$s. If ISK modulates a binary data in $n_{slice} = 128$ number of baseband symbols, the maximum throughput is $T_{max} = \frac{48}{4 \times 10^{-6} \times 128} = 93.75$ Kbps. Table II shows the maximum throughput of ISK for different slice size for two types of WiFi standards.

The observed throughput, however, will depend on the symbol error rate (SER) and can be calculated as $T_{obs} = T_{max} \times SER$.

IV. Performance evaluation

In this section, we present the performance of ISK showing: (1) the impairments classification accuracy is not influenced by variation in wireless channel conditions (Sec. IV-A); (2) it achieves a throughput of $\sim$ 93 Kbps for SNR$>$ 15dB with potential increase up to 1500 Kbps without compromising on the BER performance of a WiFi receiver (Sec. IV-B).

Experiment setup: We first identify a set of 16 impairments which generates unique patterns as discussed in Sec. II-A. Next, we collect demodulated data from WiFi packets that are transmitted over a cable from a single radio, after introducing these impairments through GNU Radio API. We replicate and augment demodulated data by adding a random Gaussian noise of power -13dB. Finally, we train the classifier with the augmented dataset using the same CNN architecture as described in Sec. II-B.

A. Classification accuracy with different channel conditions

We test the performance of the trained CNN classifier with NI X310 SDRs introducing 16 impairments. To do so, we first collect samples from the radio for all 16 impairments through cable, one pre-set impairment at a time. ISK easily distinguishes impairments that are intentionally introduced by achieving a classification accuracy of 99.76%. This indicates that our pre-trained classifier is able to identify the hardware impairments accurately.

Next, we evaluate the performance of ISK with data collected over the wireless channel. To show robustness to variation in channel conditions, we conduct the experiments in two different locations: (1) our lab, which represents a typical in-indoor environment and (2) a more open recreation area which has fewer reflections, with Tx-Rx separation distance of 8ft in both locations. The confusion matrix of classification accuracy is shown in Fig. 5a and Fig. 5b respectively. In general, in both environments ISK can achieve higher than 99.5% accuracy, which proves that the unique patterns created by the impairments can be detected even with random noise.

B. Covert communication using ISK

We evaluate symbol-error-rate (SER) and throughput performance of our proposed ISK based covert channel with the data collected over the air for X310 radio in-indoor environment. In our experimental evaluation, the radio supports all 16 impairments satisfying the BER constraint of 10^{-4}. For the transmitter radio, a receiver first randomizes these 16 impairments and then finds $^{16}P_2 = 240$ different permutations. It selects the first $2^V = 128$ permutations where $V = \lfloor (\log_2(^{16}P_2) \rfloor = 7$ to generate a table where each entry is a pair of impairments to be used to convey binary 0 or 1. We assume the receiver shares this table along with a unique generator polynomial, initial seed and a initial impairment pair to be used over a secure feedback channel. We perform $10,000$ trials to evaluate the performance. In each trial, the transmitter generates ISK packet with binary '`Preamble`' sequence of length 17, a PN binary sequence ('`ID`') of length 31 and random '`Covert Data`' of 100 bits. The transmitter uses a shared generator polynomial and random initial seed to produce a PN binary sequence, that is exactly identical to a sequence generated by the receiver.

The transmitter refers its pairwise impairment table to map each binary value 0 or 1 in the ISK encoded packet to the impairment as: $\{0 \rightarrow I_k, 1 \rightarrow I_l\}$ for a n_{slice} number of baseband symbols. We generate a new pairwise impairments table in each trial. We choose the value of n_{slice} same as the input slice length used by ISK' CNN classifier. The receiver uses trained classifier described in Sec. II-B to obtain the sequence of impairments, which are then demapped to a binary sequence. After detecting start of the packet by correlating with `Preamble` sequence, the receiver extracts the binary sequence in `ID` and matches with the output of its own PN generator to authenticate the transmitter. Only after successful authentication, the receiver decodes the `Covert Data`. In each trial, we repeat the process 10 times, where the transmitter creates a new ISK packet and changes its `ID` by generating new PN binary sequence.

We evaluate the SER of covert channel against normalized signal-to-noise (SNR) ratio $\frac{E_s}{N_0}$ with the data collected in-indoor location, where we fixed the energy per symbol to

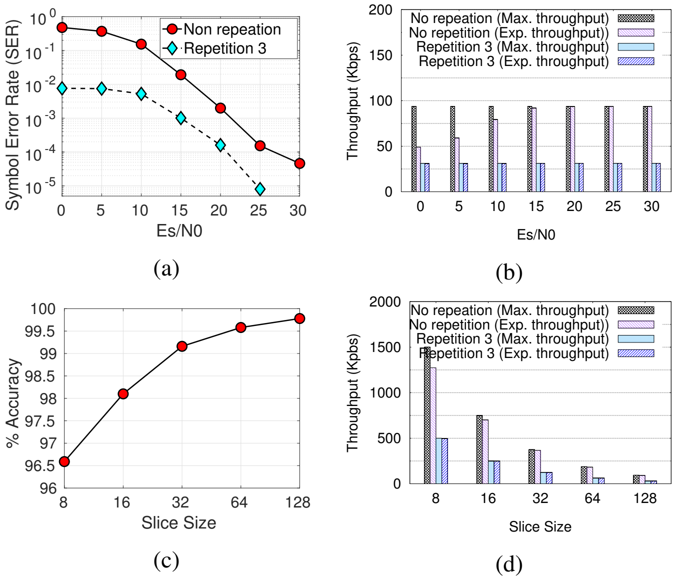


Figure 6: (a) Symbol error rate as a function of SNR $\frac{E_s}{N_0}$ for slice size of 128 b) Covert channel throughput as a function $\frac{E_s}{N_0}$ for slice size of 128 c) ISK's CNN classification accuracy as a function of slice size d) Throughput as a function slice size n_{slice} for fixed $\frac{E_s}{N_0}$ = 15dB.

E_s = 1J and varied N_0 from 0 to 30dB. Results were averaged over 10000 independent trials. As shown in Fig. 6a, ISK achieves SER $< 10^{-4}$ for SNR$>$ 25dB. To improve the SER, we propose a simple repetition technique, in which the transmitter introduces the same impairment for $n_{rep} \times n_{slice}$ number of baseband symbols, where n_{rep} is the number of repetitions. With $n_{rep} = 3$, the SER drops significantly.

Fig. 6b depicts the throughput of ISK's covert channel as a function of $\frac{E_s}{N_0}$. With increase in $\frac{E_s}{N_0}$, the achieved throughput also increases as expected. The throughput of repetition scheme is simply calculated as $T_{rep} = \frac{T}{n_{rep}}$. Although throughput achieved with repetition scheme is very low compared to no repetition, the scheme performs well in low SNR region.

Fig. 6c shows ISK's classification accuracy for different length of input slice size. This is to show that input of a smaller slice size can enable communication if we introduce artificial impairments. Fig. 6d shows the throughput for fixed $\frac{E_s}{N_0}$ = 15dB as a function of slice size n_{slice}. It is evident that ISK can increase throughput by using shorter slice size n_{slice}. However, with increase in number of impairments, the classification accuracy of identifying correct impairment will drop, motivating the need of longer slice size. Therefore, the choice of slice size is determined by the number of feasible impairments. Even though, communication requires only two impairments, the more number of pairwise impairments will lead to better security. Therefore, there is a tradeoff between the desired throughput and security while selecting the n_{slice}.

V. Conclusions

We have presented ISK, a technique that embeds a covert information in a regular WiFi transmission by introducing controlled impairments to the radio transmitter. We have proposed deep CNN architecture that is trained to decode binary 0 or 1 acting as a low-overhead classifier. We have extensively evaluated ISK's performance on a experimental testbed of X310 radios. Experimental results have shown that ISK achieves throughput of $\sim$ 93 Kbps for SNR $>$ 15dB that can be improved up to 1500 Kbps with smaller slice sizes.

Acknowledgment

This work is supported by DARPA under RFMLS program contract N00164-18-R-WQ80.

References

[1] Verizon Enterprise, "2019 Data Breach Investigations Report." https://enterprise.verizon.com/resources/reports/dbir/, 2019.

[2] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4829–4842, Dec 2018.

[3] T. Banerjee, K. R. Chowdhury, and D. P. Agrawal, "Using polynomial regression for data representation in wireless sensor networks," *International Journal of Communication Systems*, vol. 20, no. 7, pp. 829–856, 2007.

[4] K. Szczypiorski and W. Mazurczyk, "Hiding Data in OFDM Symbols of IEEE 802.11 Networks," in *IEEE Intl. Conference on Multimedia Information Networking and Security*, 2010, pp. 835–840.

[5] Z. Hijaz and V. S. Frost, "Exploiting OFDM Systems for Covert Communication," in *IEEE MILCOM*, 2010, pp. 2149–2155.

[6] R. P. Hudhajanto, I. G. P. Astawa, and A. Sudarsono, "Covert Communication in MIMO-OFDM System using Pseudo Random Location of Fake Subcarriers," *EMITTER International Journal of Engineering Technology*, vol. 4, no. 1, pp. 150–163, 2016.

[7] J. Classen, M. Schulz, and M. Hollick, "Practical Covert Channels for WiFi Systems," in *IEEE Conference on Communications and Network Security (CNS)*, 2015, pp. 209–217.

[8] S. Grabski and K. Szczypiorski, "Steganography in ofdm symbols of fast ieee 802.11 n networks," in *2013 IEEE Security and Privacy Workshops*. IEEE, 2013, pp. 158–164.

[9] K. Sankhe, U. Muncuk, M. Y. Naderi, and K. Chowdhury, "Talking when no one is listening: Piggybacking city-scale iot control signals over lte," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 1547–1555.

[10] M. Y. Naderi, K. R. Chowdhury, S. Basagni, W. Heinzelman, S. De, and S. Jana, "Experimental study of concurrent data and wireless energy transfer for sensor networks," in *2014 IEEE Global Communications Conference*. IEEE, 2014, pp. 2543–2549.

[11] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret Agent Radio: Covert Communication through Dirty Constellations," in *International Workshop on Information Hiding*. Springer, 2012, pp. 160–175.

[12] S. D'Oro, F. Restuccia, and T. Melodia, "Hiding Data in Plain Sight: Undetectable Wireless Communications Through Pseudo-Noise Asymmetric Shift Keying," in *IEEE INFOCOM*, 2019.

[13] M. Schulz, J. Link, F. Gringoli, and M. Hollick, "Shadow Wi-Fi: Teaching Smartphones to Transmit Raw Signals and to Extract Channel State Information to Implement Practical Covert Channels over Wi-Fi," in *ACM Mobisys*, 2018, pp. 256–268.

[14] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "ORACLE: Optimized Radio clAssification through Convolutional neuraL nEtworks," in *IEEE INFOCOM*, 2019.

[15] F. Restuccia and T. Melodia, "Big Data Goes Small: Real-Time Spectrum-Driven Embedded Wireless Networking through Deep Learning in the RF Loop," in *IEEE INFOCOM*, 2019.

[16] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 146–152, 2018.

[17] T. J. O'Shea and J. Corgan, "Convolutional radio modulation recognition networks," 2016. [Online]. Available: http://arxiv.org/abs/1602.04105

[18] A. Selim, F. Paisana, J. A. Arokkiam, Y. Zhang, L. Doyle, and L. A. DaSilva, "Spectrum monitoring for radar bands using deep convolutional neural networks," in *IEEE GLOBECOM 2017*.