This article has been accepted for publication in IEEE Journal of Radio Frequency Identification. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JRFID.2024.3379189

Carrier-Free RFID: Using Modulated Noise Communication to Read UHF RFID Tags

Shanti Garman*, Ali Saffari*, Daisuke Kobuchi‡, Dara Stotland†, Joshua R. Smith*†, and Zerina Kapetanovic§
*Department of Electrical and Computer Engineering, University of Washington, Seattle, WA, USA
†Allen School of Computer Science and Engineering, University of Washington, Seattle, WA, USA
‡Graduate School of Engineering, University of Tokyo, Tokyo, Japan
§Department of Electrical Engineering, Stanford University, Stanford, CA, USA

***Abstract*—In this work, we demonstrate that it is possible to read UHF RFID tags without a carrier. Specifically, we introduce an alternative reader design that does not emit a carrier and allows reading RFID tags intended for conventional carrier-based systems. While traditional RFID tags modulate a carrier, it is important to note that a modulation circuit used for backscatter also modulates the inherent noise of the tag circuitry, including the Johnson noise, irrespective of whether a carrier is present or not. Our Modulated Noise Communication (MNC) approach leverages recent work on Modulated Johnson Noise (MJN) and can be read by an alternative RFID reader design that enables simpler, more accessible RFID readings than a conventional backscatter reader by eliminating self-jamming obstructions. MNC is shown to support wireless transmission of data packets between 2 cm to 10 cm of separation between a standard UHF RFID tag and the proposed alternative reader for data rates of 1 bps and 2 bps.**

***Index Terms*—modulation, backscatter, RFID, Johnson noise, modulated noise, thermal noise**

I. Introduction

Modulated Backscatter (MBS) is a communication technique commonly used in RFID systems. It involves the selective reflection or absorption of a radio frequency (RF) signal by switching between matched (absorptive) and mismatched (reflective) impedance states [1]. Traditional RFID systems use passive wireless tags to transmit information. By relying on a generated RF carrier signal emitted by an RFID reader, a tag can either absorb the incident energy through its energy harvester circuitry or reflect ("backscatter") the incident energy to transmit information. Such systems enable wireless transmission of information without the need for batteries [2], [3]. This approach enables RFID tags to be low-power, compact, and battery-free. Ambient Backscatter (ABS) communication builds on these techniques and reduces power requirements even further by using ambient RF signals instead of a generated RF signal from a reader. Ambient sources such as over-the-air TV, FM radio, and even Wi-Fi can be used. In ABS, a passive tag harvests energy from the ambient signal and backscatters that same signal to communicate with another nearby tag or base station [4]–[6]. Applications of these concepts include supply chain management (e.g., tracking products from source to consumer), highway toll collection systems, and livestock monitoring systems using implantable RFID chips.

However, current backscatter-based systems have limitations. One challenge is their reliance on generated or ambient RF sources. These systems require passive tags to be in close proximity to an RFID reader or an existing RF source, like a TV broadcast tower, which restricts their application space. Furthermore, RFID readers are expensive and involve complex hardware to address issues such as self-jamming. Recent research has demonstrated the possibility of modulating information bits without using a generated RF signal [7]. Instead, information bits are modulated by manipulating the Johnson (thermal) noise in an unpowered resistor by selectively switching the data transmitter between an impedance-matched resistor and an open (or short) circuit. Johnson noise has previously been explored for use in computing and in quantum key distribution schemes [8], [9]. Additional work explores the use of extraterrestrial noise sources [10].

Building on this, our previous research showed the extension of Modulated Johnson Noise (MJN) to RFID tags by implementing Modulated Noise Communication (MNC) [11]. Using a standard WISP 6.0 tag, we demonstrated that unmodified RFID tag hardware can transmit information bits wirelessly by modulating the noise inherent to the tag's circuitry, without the need for an RF carrier. Although the RFID tag was originally designed for modulating a backscattered carrier, we proved that the tag's backscattering circuitry effectively modulates the intrinsic noise of the tag, despite not being explicitly designed for this purpose. To receive the modulated noise data, an alternative receiver (i.e., an alternative RFID reader) is required. As described in [11], a MJN or MNC reader is much simpler than a conventional RFID reader, because it does not need to generate a carrier signal and hence does not need to employ measures to counteract self-jamming.

While prior work demonstrated promising results for extending MNC to RFID tags, the experimental results were based on a small number of packet transmissions, and system characterization was presented at a high level. This paper aims to improve the understanding of the proposed system and its capabilities by providing deeper discussion and a more extensive characterization of the system. Primary contributions of this work include: **(1)** We share experimental results for a larger number of packet transmissions at various distances and

This work supported in part by NSF award CNS-1305072.

This article has been accepted for publication in IEEE Journal of Radio Frequency Identification. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JRFID.2024.3379189

data rates. Specifically, we present results from 900 wireless packet transmissions, compared to prior results which were based on approximately 50 wireless packet transmissions. **(2)** We demonstrate that unmodified RFID tags can be used to wirelessly transmit information bits at a distance of 10 cm and a data rate of 2 bps. This represents an increase over previously published results of 5x and 2x for achievable distance and data rate, respectively. **(3)** We present and discuss important system-level optimizations which enable the improved performance demonstrated here.

II. Physical Principles of Johnson Noise

Johnson noise, or thermal noise, is the thermal agitation of charge carriers (e.g., electrons) inside an electrical conductor, such as a resistor [12], [13]. As described in [7] and [11], this thermal noise is present in any circuit element with a real impedance, even without applying external source voltage or current. Johnson noise is also shown to be broadband or "white" at frequencies below 6 THz. The only dissipative (resistive) elements in the WISP analog front end are the diodes, which can be thought of as resistors for the purpose of modeling Johnson noise. A diode can be thought of as a resistor whose value changes with current. Different parts of the diode I–V curve exhibit different behavior (see Fig. 1). Three regions are shown, corresponding to different non-linear and linear behavior of a diode [14]. The reciprocal of the slope at each point on the I–V curve defines a differential resistance at that point on the curve. For our purposes, we are mainly interested in the behavior of the I–V curve at zero bias (i.e., at the origin of the I–V curve). Even though the diode acts as a non-linear (and strongly bias dependent) resistor, as explained in [15], it still produces Gaussian thermal noise at equilibrium. Thus for our purposes, it can be used in the same way as a resistor: as a source of thermal noise. Shot noise, another form of noise arising from the discreteness of electric charge, only occurs at non-zero current; since the diodes are unbiased, Johnson noise is expected to be the main noise source produced by the diodes.

Regarding impedance calculations, it is also important to note that the impedance of the diodes will vary with input power to the WISP, or any other standard RFID tag, as input power affects the biasing of the rectifying diodes. This relationship between input power and diode impedance has important implications for the input matching network, as well as for the contrast between impedance states of an RFID tag. For example, the input matching network of a standard RFID tag is typically optimized with a target input power that is specified by the RFID reader carrier signal. In this case, the diodes are forward biased, and they present a lower impedance value to which the matching network is connected. However, without a carrier signal, the diodes are unbiased, and they present a higher impedance value. If the input matching network remains unchanged, the result of this is that the overall impedance of the circuit changes. The impedance values directly affect the amount of Johnson noise power which is transmitted. This is further discussed in Section IV.

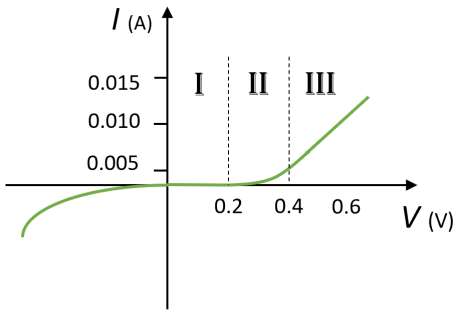


Fig. 1: **Diode as a non-linear resistor.** Typical current (I) vs voltage (V) plot ("I–V curve") for a silicon-based Schottky diode. The reciprocal slope of the I–V curve at any point defines a "differential" resistance value at that point on the curve. Regions I–III correspond to different non-linear and linear behavior [14]. While the device's non-linear and voltage dependent resistance value may change the properties of the noise (compared to a linear resistor), the key for our purpose is that it is a dissipative device and therefore a source of thermal noise.

As shown in Fig 2, the WISP 6 analog front end includes a backscatter switch (ADG902) which switches between two states: "switch closed" and "switch open." When the backscatter switch is closed, the antenna is connected through the switch to a 3.3 nF capacitor to ground, effectively shunting the input path. When the backscatter switch is open ("switch open" state), the shunt capacitor is disconnected. When the backscatter switch is closed ("switch closed" state), the circuit pathway to ground presents a low impedance (0.05 Ω at 915 MHz) which should decrease the observed noise. This is because the low impedance pathway acts like a short circuit, a typical "cold load" in MJN implementations [7], [10]. Indeed, measurements of the received noise power from a WISP in a cabled setup confirm this, and the difference in noise power in the two backscatter states enables the RFID tag to communicate by modulating this noise. Noise power measurement results are included Section IV-C.

III. System Description and Implementation

The system under investigation consists of two main components: a transmitter and a receiver. The data transmitter is built using standard RFID tag hardware and operates on a custom protocol. Specifically, we utilize version 6 of the Wireless Identification and Sensing Platform (WISP 6) [16], with no modifications made to its circuit design. Although the WISP 6 is a recent iteration of the WISP hardware, it lacks any specialized features explicitly designed for supporting Modulated Noise Communication. The necessary changes were only made to the software running on the WISP to enable Modulated Noise Communication. In its listening mode, the WISP 6 consumes an average power of 22μW, and we estimate that an accelerometer-enabled WISP 6 tag utilizing MNC would consume less than 400μW due to its lower data rate compared

This article has been accepted for publication in IEEE Journal of Radio Frequency Identification. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JRFID.2024.3379189

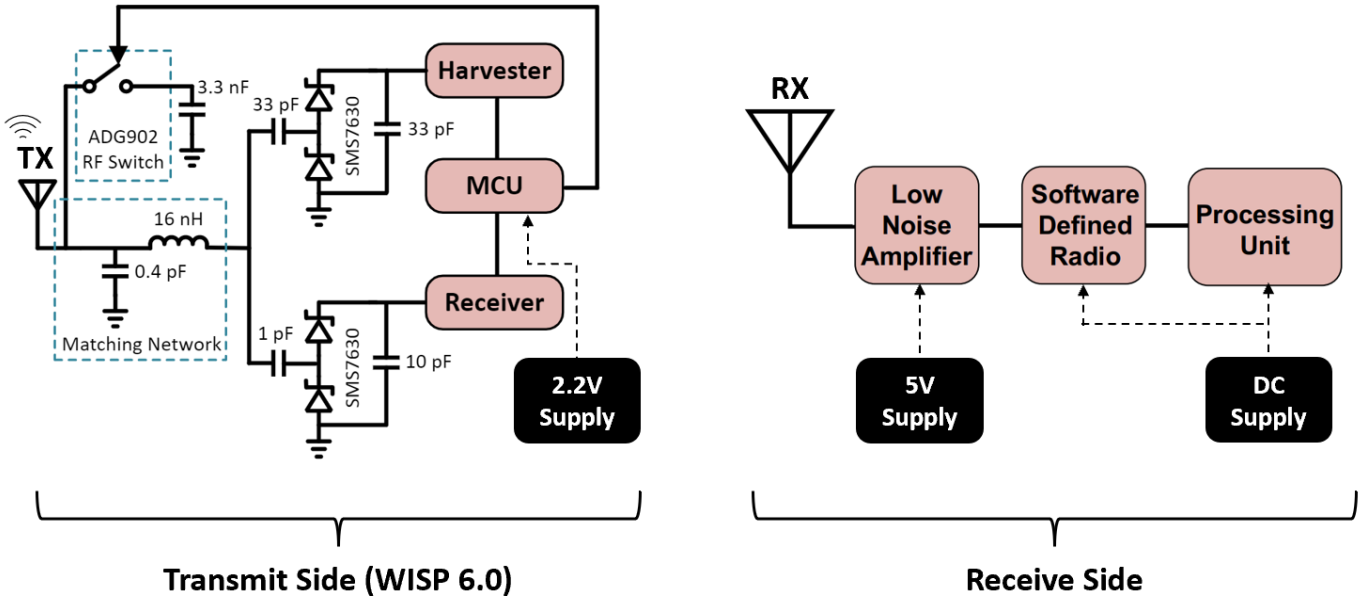


Fig. 2: **Schematic and Block Diagram of MNC System.** The transmit side consists of a standard WISP 6 tag running a custom MNC modulation protocol to control the backscatter switch. Noise inherent to the RFID tag is modulated by switching between the open and closed states. The receive side consists of a low noise amplifier (LNA), software-defined radio (SDR), and processing unit. By modulating tag noise, an RFID tag can transmit information without requiring a carrier. Thus, simplified RFID readers can be used and complex self-jamming countermeasures can be avoided.

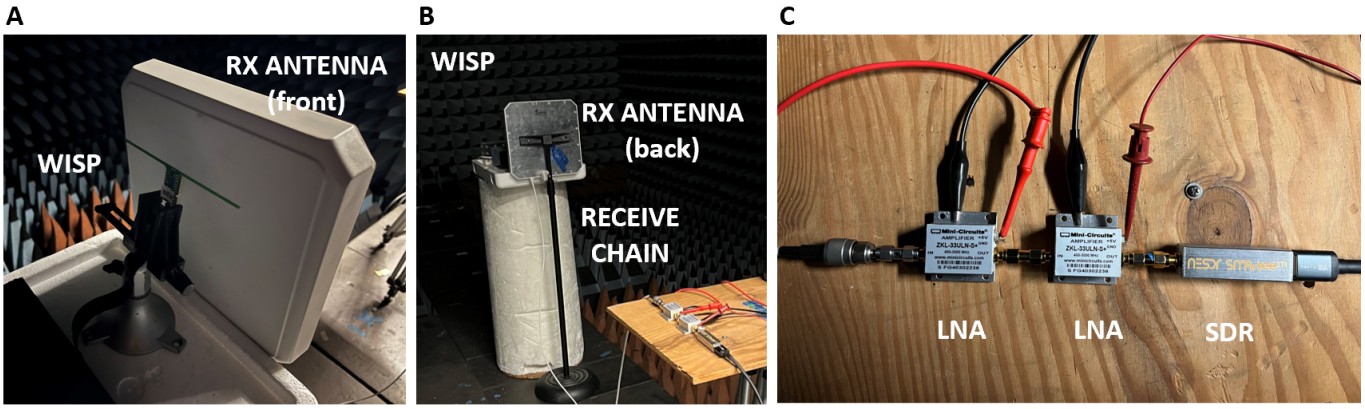


Fig. 3: **Prototype Implementation. (A)** shows the transmitter (standard WISP 6) and receive antenna (RFID patch antenna). **(B)** shows the transmit and receive components inside an anechoic chamber. **(C)** shows the remaining components in the receive chain. The patch antenna output is connected through a coaxial cable to the LNA input, and the SDR output is connected through a USB cable to the processing unit located outside of the chamber (not shown).

to a WISP in standard operation. Moreover, we anticipate that earlier versions of the WISP and other RFID tag hardware should also be capable of transmitting MNC data, given that the appropriate protocol modifications can be implemented.

The receiver component is constructed using off-the-shelf components and follows a similar design approach as described in [7]. It incorporates two Mini-Circuits ZKL-33ULN-S+ low noise amplifiers (LNAs), contributing around 70 dB of total gain [17]. This is followed by a software-defined radio (SDR) and a processing unit. In our implementation, we utilize either RTL-SDR Blog V3 or NESDR SMArTeeXTR USB-based SDRs [18], [19], while the processing unit is a laptop PC. Fig. 2 illustrates the high-level hardware design, and Figs. 3A and B showcase the prototype implementation of the system. The primary hypothesis driving this research is that the backscatter modulation circuitry of an RFID tag generally results in an impedance change between its noise-generating components and its antenna, allowing the utilization of tag hardware designed for Modulated Backscatter communication to facilitate Modulated Noise Communication.

In this work, we describe both a cabled implementation and a wireless implementation of MNC to enable transmission of data. The cabled implementation employs a WISP 6 which has been modified to replace the dipole antenna with a Sub-

This article has been accepted for publication in IEEE Journal of Radio Frequency Identification. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JRFID.2024.3379189

Miniature version A (SMA) connector and is used to validate the concept of modulating the WISP tag noise by connecting the tag's analog front end directly to the MNC receiver LNA (see Fig. 4). We also use the cabled setup to evaluate impedance and noise power when the backscatter switch is in the closed and open states. For the wireless implementation, an off-the-shelf WISP 6 is used with its standard dipole antenna intact. The MNC receiver used in the wireless setup is identical to the receiver in the cabled setup, except that a RFID antenna is connected at the MNC receiver LNA input [20]. This RFID antenna reads the modulated thermal noise signals emitted from WISP 6's integrated dipole antenna. The wireless implementation described here is the proposed approach for actually realizing carrier-free RFID. Experimental results presented in this paper for transmission of data packets over distance use the wireless implementation. Additional details on the experimental setup for all measurements are included below in the Section IV.

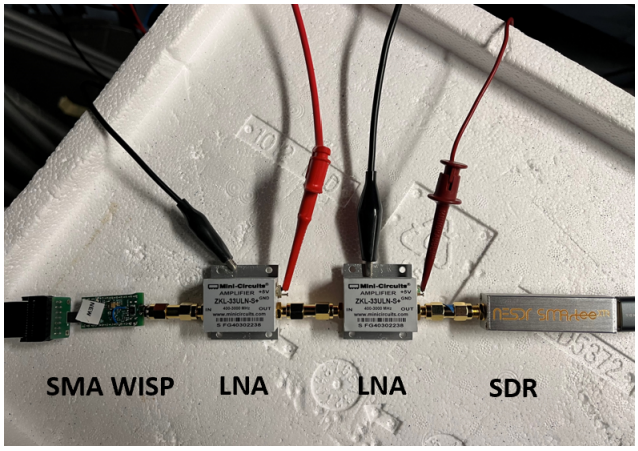


Fig. 4: **Cabled Implementation.** A WISP 6 tag is modified to replace the dipole antenna with a SMA connector enabling a direct feed to the receiver chain LNA. This setup is used to measure impedance with the tag's RF switch in "switch open" and "switch closed" states.

A. Modulation and Coding Scheme

To encode data on the transmit side and to decode data on the receive side, we employ the same ON-OFF keying scheme described in [7]. In this approach, a 1-bit is defined as the backscatter switch being "ON", i.e., continuously switching between the two impedance states, while a 0-bit is defined as the backscatter switch being "OFF", i.e., staying in its default state. The rate of switching for a 1-bit occurs at a specified subcarrier frequency. We use $f_b = 100Hz$ for all data presented here. Furthermore, each data transmission uses a 20-bit packet structure. The first 7 bits contain a preamble (Barker-7), and the remaining 13 bits are reserved for the data to be transmitted. Details about the parameters for the modulation and coding scheme used in this work are summarized in Table I. To enable transmission of the specified packet and data rate, firmware modifications are made to

Parameter	Value	Units
Center frequency	915	MHz
Subcarrier signal	Square wave, 50% duty cycle	n/a
Subcarrier frequency	100	Hz
Packet length	20	bits
Preamble length	7	bits
Preamble	"1110010"	n/a
Data length	13	bits
Data	"1010101010000"	n/a
Data rate	1 or 2	bps

TABLE I: Modulation and Coding Parameters for Transmitter

Data Rate (bps)	Number of Cycles
10	10
5	20
4	25
2	50
1	100
0.5	200

TABLE II: Required Subcarrier Cycles by Data Rate with $f_b = 100$ Hz

the WISP software. Specifically, the microcontroller code is modified to continuously transmit packets by controlling the RF switch using the subcarrier frequency as the switching frequency. As mentioned previously, a 1-bit is transmitted by continuously switching. This means that different data rates require different number of subcarrier cycles, where one cycle is simply the period of the subcarrier signal. For example, to transmit at a data rate of 1 bps, a 1-bit requires 100 cycles of switching at the subcarrier frequency, while at a data rate of 2 bps, a 1-bit requires 50 cycles (see Table II). Equation 3 describes the relationship, where the number of subcarrier cycles per bit N_c is shown as the ratio of the subcarrier frequency f_b (Hz) to data rate (bps).

$$N_c = \frac{f_b}{Data\ Rate} \tag{1}$$

The modifications to the WISP software described here are the only modifications required to enable the WISP as a MNC transmitter.

Fig. 5 illustrates the packet structure used in this work; waveform A illustrates the packet bit stream, waveform B shows the subcarrier (not to scale), and waveform C shows the resulting waveform to be transmitted, which is the convolution of the information bits of the packet (waveform A) and the subcarrier (waveform B). Fig. 6 shows a time domain measurement of the WISP which validates the packet transmissions.

To receive data, heterodyne detection is implemented. Samples are read by the SDR and integrated into in-phase (I) and quadrature (Q) accumulators. The SDR is set to sample at 1 Msps and gain of 1.5. It is assumed that the receiver is configured with the same subcarrier frequency, preamble, and data rate of the transmitted signal. However, this method of demodulation does not require synchronization of the receiver

This article has been accepted for publication in IEEE Journal of Radio Frequency Identification. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JRFID.2024.3379189

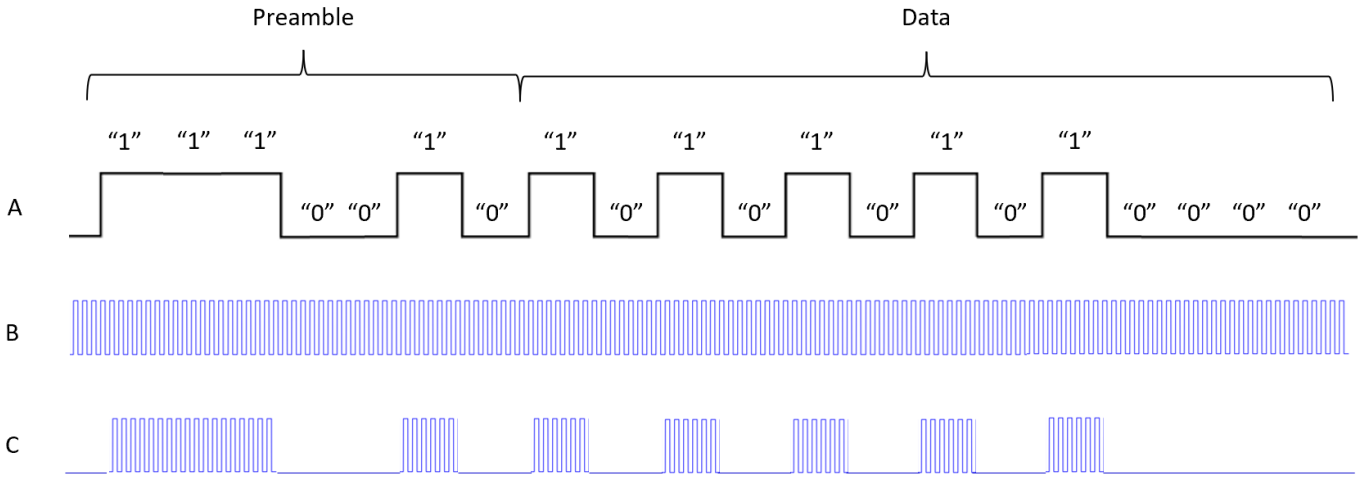


Fig. 5: **Packet Structure.** Waveform **(A)** illustrates the packet bit stream, including a 7-bit Barker preamble followed by a 13-bit data payload. **(B)** shows the subcarrier (not to scale), and **(C)** shows the resulting waveform which is the convolution of the information bits and the subcarrier. Waveform **(C)** is the final waveform to be transmitted.

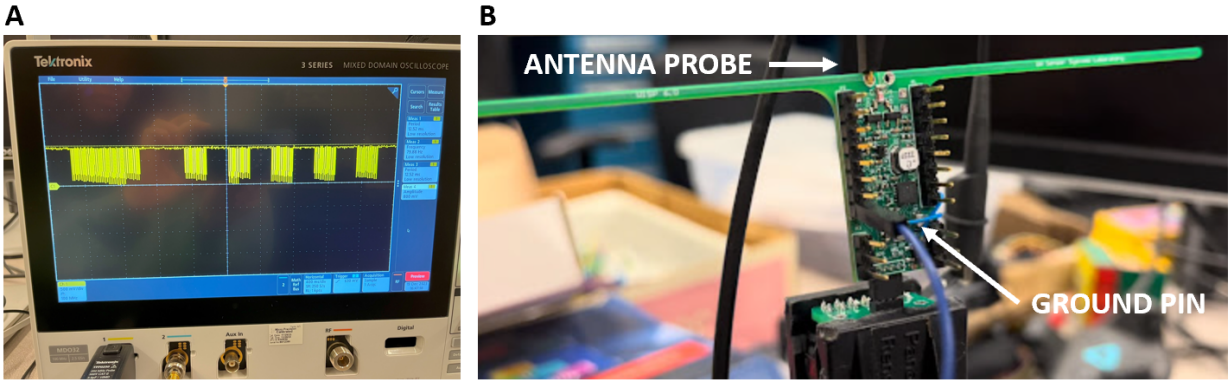


Fig. 6: **Time domain measurement of WISP transmission. (A)** Waveform is recognizable as the 7-bit barker preamble followed by the first eight bits of the 13-bit data payload. The subcarrier switching is also discernible. **(B)** Oscilloscope probe is connected to WISP antenna probe point and ground pin.

subcarrier phase and the transmitter subcarrier phase. Table III summarizes the decoding parameters used in this work for the receive side.

Parameter	Value	Units
SDR sampling rate	1	Msps
SDR center frequency	915	MHz
SDR gain	1.5	n/a
Samples per bit	2 to 7	n/a
Subcarrier frequency	100	Hz
Preamble	"1110010"	n/a
Data rate	1 or 2	bps

TABLE III: Decoding Parameters for Receiver

IV. Experimental Results

Both cabled and wireless implementations described above are evaluated in an anechoic chamber, and the results are presented in this section, following a more detailed description of the experimental setup. First, impedance measurements are presented, along with a discussion of their observed variation with input power. Noise power measurements follow, including measured noise power of reference loads, as well as measured noise power of the wireless system in each impedance state. Finally, results from wireless transmission, demodulation, and decoding of packets are presented. The system is evaluated at data rates of 1 bps and 2 bps, with the WISP configured to continuously transmit data packets at the specified data rate. Distance between the WISP and the RFID patch antenna is varied from 2 cm to 10 cm, in 1-cm increments, with 50 packets transmitted for each measurement. For each evaluation, the system operates according to the modulation and coding parameters described previously (see Tables I–III).

A. Experimental Setup

As shown in Fig. 3, the transmit and receive elements are situated inside an anechoic chamber. The purpose of this is to reduce unwanted interference from other RF sources during

This article has been accepted for publication in IEEE Journal of Radio Frequency Identification. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JRFID.2024.3379189

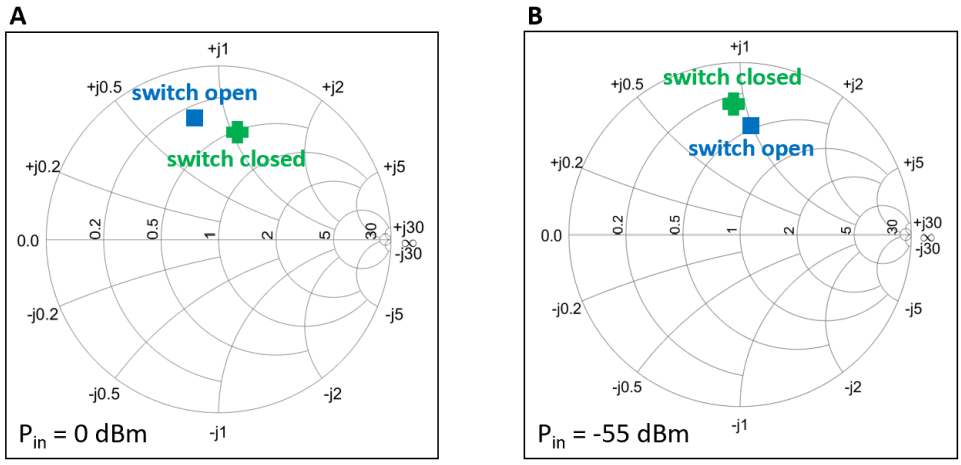


Fig. 7: **Impedance measurements at high and low stimulus levels.** A VNA is used to directly measure reflection coefficient (S_{11}) of the SMA-connectorized WISP in two impedance states at different input power levels. Normalized values are plotted on Smith charts. For **(A)** the VNA stimulus is set to $P = 0$ dBm. For **(B)** the VNA stimulus is set to $P = -55$ dBm. It is observed that the input impedance of the WISP analog front end changes according to the input power level. In **(B)**, the impedance is greater in the "switch open" state than the "switch closed" state.

system evaluation and characterization. In addition, care is taken to remove extraneous metallics from the area around the WISP and RFID patch antenna. Instead, styrofoam stands and platforms are used. This is particularly important during wireless data transmissions, as the presence of metallics is known to affect wireless signals and antenna patterns. Indeed, the presence of various metallics in prior work has been shown to affect measurements [11]. The height from the floor is approximately $h = 1.25$ m; this height helps reduce signal reflections and multipath effects from the rubber walkway on which the stands are positioned. The processing unit is located outside of the chamber, and the chamber door is closed during data collection. Data cables and power cables are routed from the equipment inside the chamber to the outside of the chamber. Finally, all RF equipment undergoes a "warm-up" period of at least 45 minutes prior to data collection.

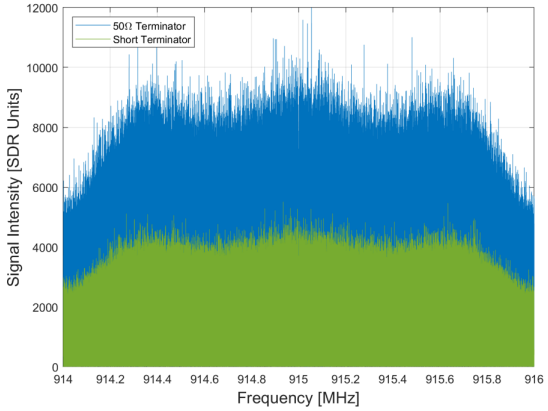
B. Impedance Measurements

A Vector Network Analyzer (VNA) is used to characterize the reflection coefficient and measure impedance of the WISP in its two states (see Fig. 7). The SMA-connectorized WISP is connected to a calibrated VNA to directly measure reflection coefficient (S_{11}) of the two impedance states. Measurements are made at two different input power levels, since the impedance of the diodes is dependent on the input power. Specifically, the VNA stimulus is set to $P = 0$ dBm and $P = -55$ dBm. $P = -55$ dBm is at the low end of the VNA stimulus power range, and this value is selected to better simulate the absence of a generated RF signal at the WISP input. As seen in Figs. 7A and 7B, the change in input power level results in a change to the input impedance of the WISP analog front end. Measured impedance values are plotted on a Smith chart normalized to a characteristic impedance of $Z_0 = 50\ \Omega$. At $P = 0$ dBm, measured impedance values are $z_{switchopen,A} = 0.28 + j0.78\ \Omega$ and $z_{switchclosed,A} = 0.51 + j1.06\ \Omega$. At $P = -55$ dBm, measured impedance values are $z_{switchopen,B} = 0.47 + j0.98\ \Omega$ and $z_{switchclosed,B} = 0.26 + j0.92\ \Omega$. As Fig. 7B shows, for a very low input power level, the impedance is greater in the "switch open" state than the "switch closed" state. With no external RF carrier, the WISP operating as a MNC transmitter is expected to have impedance values similar to these.

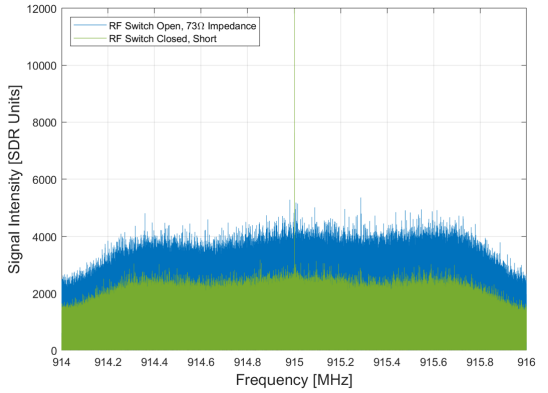
C. Noise Power Measurements

Noise power is recorded with different input sources, including known "hot" and "cold" loads such as 50 Ω, Short, and Open terminators [7], as well as the WISP, at the input to the receive chain. We measure the noise power with the WISP in each impedance state: "switch open" and "switch closed." These measurements are used to validate our hypothesis that the two states will yield different levels of received noise power. A 60-second recording is made using the SDR to capture raw IQ data with the WISP fixed in each state and with all receiver components powered on. The noise power spectrum from the raw data is found by performing a Fast-Fourier Transform (FFT). The resulting noise power at the frequency of interest is plotted in Fig. 8. Fig. 8A shows the contrast in received noise power from a "hot" load (50 Ω terminator) and a "cold" load (Short terminator). The noise power with the 50 Ω terminator is greater than the noise power with the Short terminator, which is consistent with prior work [7], [10]. Fig. 8B illustrates the contrast in received noise power from the WISP in its two impedance states. It is observed that the noise power when the WISP is in the "switch open" state is larger than the noise power when the WISP is in the "switch closed" state, as expected. Although the absolute magnitudes of the noise power with the WISP is lower than the noise power with the discrete terminators connected directly to the receive chain, the relative magnitudes of the noise power in the two states is consistent with expected results. Furthermore,

This article has been accepted for publication in IEEE Journal of Radio Frequency Identification. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JRFID.2024.3379189



(a) Noise power in cabled implementation with 50Ω and Short terminators.



(b) Noise power in wireless implementation from two impedance states: "switch open" and "switch closed."

Fig. 8: **Noise power measured with various input "hot" and "cold" sources. (A)** shows a 50 Ω terminator and Short terminator are each connected directly to the receive chain. Noise power with 50 Ω is greater than noise power with Short, consistent with prior work [7], [10]. For **(B)** noise power is measured with the wireless implementation with the WISP in the "switch open" and "switch closed" states. Noise power in the "switch open" state is greater than noise power in the "switch closed" state. Contrast between the noise power in the two states enables modulation of this noise.

contrast between the states is evident. As described previously, this difference in noise power in the two states enables the WISP to communicate by modulating this noise.

D. Data Transmission, Detection, and Decoding

Contrast between the two impedance states suggests encoding data by modulating tag noise should be possible. To evaluate packet transmission, the WISP is set to transmit a 20-bit packet as described above via Modulated Noise Communication with a 100 Hz subcarrier frequency.

Raw IQ data from the SDR centered at 915 MHz with sampling frequency of 1 Msps is received, recorded, and decoded using the same coding parameters described above. Various data rates and distances are evaluated, including data rates of 1 bps and 2 bps over distances of $d = 2$ cm to $d = 10$ cm. Robust testing at data rates above 2 bps and distances beyond 10 cm are not included in this study. Evaluation over range starts with the WISP positioned very close to the receive patch antenna ($d = 2$ cm), and distance is incremented by 1 cm up to a distance of $d = 10$ cm. To ensure robust evaluation, 50 packets are sent for each measurement. Sample decoded packets for $d = 2$ cm are shown in Figs. 9A and 9B for data rates of 1 bps and 2 bps, respectively. As shown in Table IV, packets are transmitted and decoded with a high degree of accuracy, achieving a bit error rate (BER) below 1.00% and zero packet loss, from $d = 2$ cm to $d = 7$ cm for both data rates. As distance increases from $d = 8$ cm to $d = 10$ cm, packet loss increases, with more packets lost at the higher data rate and greatest distances, as expected. Fig. 10 illustrates the experimental results graphically; Fig. 10A shows the results at a data rate of 1 bps, and Fig. 10B shows the results at a data rate of 2 bps.

It is worth noting that the theoretical boundary between the reactive near-field and radiating near-field occurs within this range, at approximately $d = 7.2$ cm for the WISP dipole antenna at 915 MHz, per Equation 2,

$$R_1 = 0.62\sqrt{D^3/\lambda} \tag{2}$$

where R_1 is the boundary between the reactive near-field region and the radiating near-field region, also known as the Fresnel region [21]. The far-field distance is approximately $r_{ff} = 16.4$ cm following Equation 3,

$$R_2 = 2D^2/\lambda \tag{3}$$

where R_2 is the boundary between the radiating near-field region and the radiating far-field region, also known as the Fraunhofer region. In Eqns. 2 and 3, D is the length of the WISP dipole antenna, and λ is the free-space wavelength at the resonant frequency.

All measurements reported in this work are in the near-field, but measurements between $d = 2$ cm to approximately $d = 7$ cm are in the reactive near-field region while measurements between $d = 7$ cm to $d = 10$ cm occur in the radiating near-field region. Further characterization of the system in the reactive near-field and radiating far-field regions is a recommended step for future work. Furthermore, while distances beyond $d = 10$ cm are not evaluated in this work, it is expected that wireless transmission of data at 1 bps and 2 bps should be feasible beyond 10 cm. Characterization of packet loss and BER at greater distances is recommended.

V. Future Work

We present several future research directions to promote further investigation and optimization for enabling RFID tags to communicate by means of modulating Johnson noise. Recent work shows promise in this area, including the additional results and demonstrations of MNC presented here. Key areas for future work include:

This article has been accepted for publication in IEEE Journal of Radio Frequency Identification. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JRFID.2024.3379189

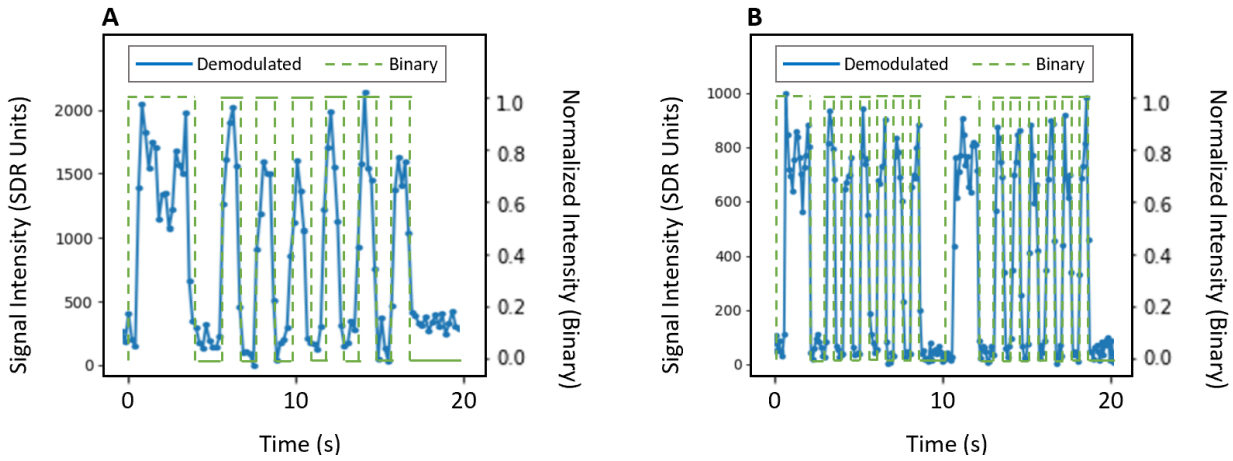


Fig. 9: **Demodulated packets for wireless implementation.** Data sent by WISP 6 via Modulated Noise Communication is demodulated successfully at **(A)** 1 bps and **(B)** 2 bps over distances from $d = 2$ cm (shown above) up to $d = 10$ cm.

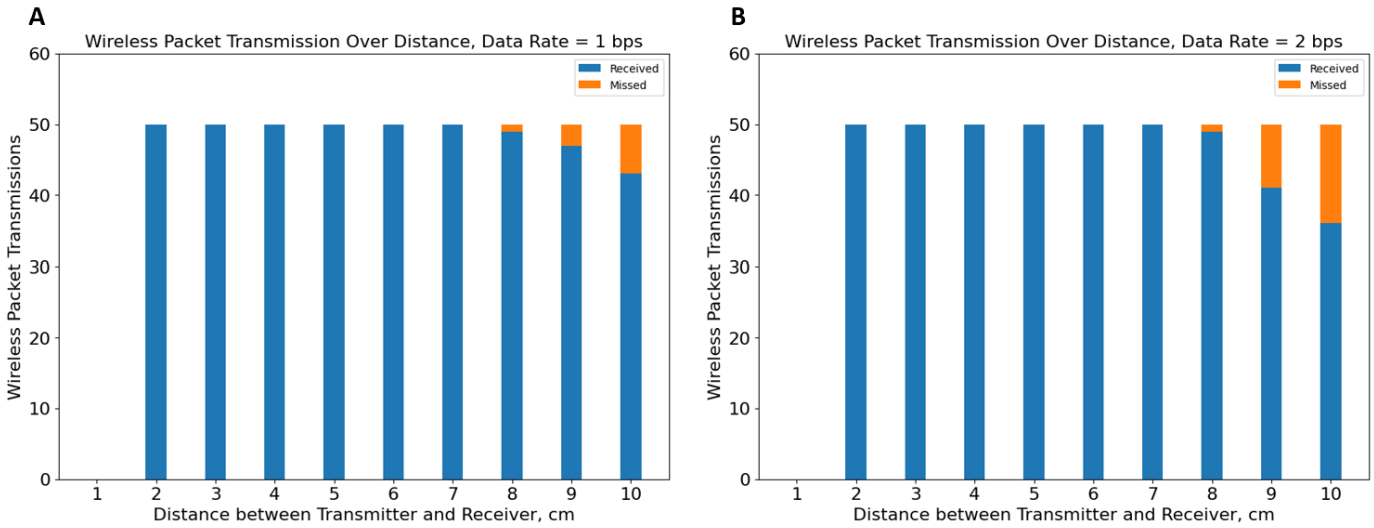


Fig. 10: **Packet transmissions achieved for wireless implementation at 1 bps and 2 bps over distances from 2 cm to 10 cm. (A)** shows results for a data rate of 1 bps, and **(B)** shows results for a data rate of 2 bps. Both data rates demonstrate perfect performance for a large volume of packets from $d = 2$ cm to $d = 7$ cm. At greater distances, from $d = 8$ cm and $d = 10$ cm, some packet loss occurs, with the higher data rate transmissions experiencing more packet loss than the lower data rate transmissions. See Table IV for detailed bit error rate and packet loss data.

- **Applications:** Building and testing applications of the technology, such as communication with smart cards, with wearable sensors, or with implanted devices, will help refine and mature the technology. This will require either integrating with energy harvesting devices, or building a custom RFID reader that time multiplexes between an RF powering mode and a thermal noise communication mode. Building the custom reader will help test our hypothesis that modulated noise communication can enable less expensive RFID systems.
- **Noise Source Evaluation:** It is hypothesized that the primary source of thermal noise on the WISP is the diodes, as these are the only resistive components in the analog front end of the WISP. While the noise power and impedance measurements presented above confirm contrast between the path with the diodes ("switch open") and the shunt path bypassing the diodes ("switch closed"), additional work is recommended to further validate this hypothesis. For example, direct measurements of the standalone diodes, isolated from other circuitry, would help validate their role as sources of thermal noise.
- **RF Switch Optimization:** It is known that different RF switches contain variations in internal circuitry. For example, the ADG902 backscatter switch used in the WISP 6 is a reflective switch, while its companion version the ADG901 is absorptive and includes 50Ω shunts at both RF ports. Furthermore, the specific impedance due to a given RF switch could lead to different results and could potentially

Data Rate	Distance	Packets Sent	Packets Received	Bit Error Rate	Packet Loss
bps	cm	#	#	%	%
1	2	50	50	0.00	0.00
1	3	50	50	0.00	0.00
1	4	50	50	0.00	0.00
1	5	50	50	0.00	0.00
1	6	50	50	0.00	0.00
1	7	50	50	0.30	0.00
1	8	50	49	0.46	2.00
1	9	50	47	2.00	6.00
1	10	50	43	0.50	14.00
2	2	50	50	0.00	0.00
2	3	50	50	0.00	0.00
2	4	50	50	0.00	0.00
2	5	50	50	0.00	0.00
2	6	50	50	0.00	0.00
2	7	50	50	0.00	0.00
2	8	50	49	0.00	2.00
2	9	50	41	3.36	18.00
2	10	50	36	5.50	28.00

TABLE IV: Summary of Wireless Data Transmissions

improve performance. Thus, exploring different RF switch options can offer insights into optimization possibilities.

- **Evaluating Throughput:** While this work focuses on limited data rates of 1 bps and 2 bps, and tests a single packet structure, it would be beneficial to evaluate bit error rate (BER) and packet error rate (PER) for complex packets at higher data rates. Comparing performance metrics between cabled and wireless implementations would facilitate further optimization efforts.
- **Communication Range:** Prior work assessed performance variation of a wireless implementation as distance between the transmitter and receiver was increased [11]. The implementation used the same wireless receiver described in this paper. However, in place of the standard WISP 6 as the wireless transmitter, a transmitter was implemented by connecting the SMA WISP to a RFID patch antenna. Distance between the two patch antennas was varied from $d = 15$ cm to $d = 45$ cm, and SDR intensity was measured at 5-cm increments. As expected, intensity mostly decreased as the separation distance increased. However, the implementation did not use the standard WISP and did not assess transmission of information bits. These are two areas of future work related to communication range.
- **Evaluating Feedthrough:** To ensure reliable performance, it is essential to investigate feedthrough from the switch control signal. Previous research [7] demonstrated the absence of modulated signals when identical loads were used, indicating no feedthrough. To verify that feedthrough is not present in this implementation of the WISP tag, it may be necessary to modify the circuit board to create identical loads for the "switch open" and "switch closed" states in future work.

VI. Conclusion

In this research paper, we present promising findings that demonstrate the feasibility of RFID communication without a carrier. Instead, wireless communication is achieved by modulating the inherent noise of the tag itself. Communicating by modulating Johnson (thermal) noise is theoretically interesting from the perspective of both communications and thermodynamics. Although our work utilizes the WISP 6 RFID tag, we believe that the hardware of most RFID tags can support MNC due to the necessity of modulating impedance to implement backscatter. This modulation generally affects thermal or other noise sources in the tag. Furthermore, it seems that specific design parameters would need to be delicately balanced in order to actually prevent MNC. For example, if the two impedance states produce different levels of thermal noise while the two switch states produce noise that precisely cancels out the difference in thermal noise. However, it is highly likely that the capability to communicate data via MNC is inherent in a variety of backscatter hardware, making it challenging to design backscatter tags that cannot support MNC without specific design choices.

The practical impact of this work is difficult to predict, but some potential ideas are considered here. One can imagine that a new type of RFID tag could be designed that relies on MNC for its uplink communication. Such a system would allow the use of less complex and more cost-effective readers, as they would not need to overcome self-jamming. Another possibility is the design of hybrid tags that can be read by both conventional RFID readers and MNC readers. In fact, our research demonstrates that the existing analog front end of a standard RFID tag can support MNC, meaning that MNC capabilities could easily be added to an existing tag design by simply modifying the digital portion (or if applicable, as in the case for the WISP) the tag's software.

If one were to design a hybrid MBS/MNC RFID tag or an MNC-only RFID tag, it would be necessary to consider different modulation circuitry than what is presented in this paper, which focuses on a MBS tag design which is capable of MNC communication. Since the range of MNC is expected

to be shorter than that of MBS, it is most likely to be suitable for short-range applications such as so-called "proximity tags" used in credit cards, building access cards, and transportation systems.

Another potential application lies in implantable and wearable bio-sensors. In these cases, the absence of a carrier has the advantage of minimizing RF exposure to the patient's body. However, a separate power source other than the RF carrier would be required for this benefit. Our proposal to time multiplex between RF power and modulated noise communication does not offer this advantage.

It is worth noting that under certain circumstances, MNC could potentially enable new side-channel attacks on backscatter devices. Addressing this potential vulnerability would involve designing careful countermeasures that balance the differences in thermal noise, which are commonly present in backscatter, with "masking" noise sources to eliminate the contrast between backscatter states. Alternatively, it may be possible to design a backscatter modulator that presents the same real impedance and consequently the same thermal noise to the antenna in both impedance states.

REFERENCES

[1] H. Stockman, "Communication by means of reflected power," *Proceedings of the IRE*, vol. 36, no. 10, pp. 1196–1204, 1948.

[2] A. P. Sample and J. R. Smith, "The wireless identification and sensing platform," *Wirelessly powered sensor networks and computational RFID*, pp. 33–56, 2013.

[3] AtlasRFIDStore, "Impinj Speedway Revolution R420 UHF RFID Reader." Downloaded from https://www.atlasrfidstore.com/impinj-speedway-revolution-r420-uhf-rfid-reader-4-port/.

[4] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," *ACM SIGCOMM computer communication review*, vol. 43, no. 4, pp. 39–50, 2013.

[5] A. Wang, V. Iyer, V. Talla, J. R. Smith, and S. Gollakota, "FM Backscatter: Enabling Connected Cities and Smart Fabrics.," in *NSDI*, vol. 17, pp. 3154630–3154650, 2017.

[6] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith, "Passive Wi-Fi: Bringing low power to Wi-Fi transmissions," in *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, pp. 151–164, 2016.

[7] Z. Kapetanovic, M. Morales, and J. R. Smith, "Communication by means of modulated Johnson noise," *Proceedings of the National Academy of Sciences*, vol. 119, no. 49, p. e2201337119, 2022.

[8] L. B. Kish, "Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law," *Physics Letters A*, vol. 352, no. 3, 2006. https://doi.org/10.1016/j.physleta.2005.11.062.

[9] L. Gunn, A. Allison, and D. Abbott, "A directional wave measurement attack against the Kish key distribution system," *Nature Scientific Reports*, vol. 4, no. 6461, 2014. https://doi.org/10.1038/srep06461.

[10] Z. Kapetanovic, S. Garman, D. Stotland, and J. R. Smith, "Cosmic backscatter: New ways to communicate via modulated noise," in *Proceedings of the 22nd ACM Workshop on Hot Topics in Networks*, pp. 165–171, 2023.

[11] S. Garman, A. Saffari, D. Kobuchi, J. R. Smith, and Z. Kapetanovic, "Modulated Noise Communication: Reading UHF RFID tags without a carrier," in *2023 IEEE International Conference on RFID (RFID)*, pp. 19–24, IEEE, June 2023.

[12] H. Nyquist, "Thermal agitation of electric charge in conductors," *Phys. Rev.*, vol. 32, pp. 110–113, Jul 1928.

[13] J. B. Johnson, "Thermal agitation of electricity in conductors," *Phys. Rev.*, vol. 32, pp. 97–109, Jul 1928.

[14] A. Boaventura, A. Collado, N. B. Carvalho, and A. Georgiadis, "Optimum behavior: Wireless power transmission system design through behavioral models and efficient synthesis techniques," *IEEE Microwave Magazine*, vol. 14, pp. 26–35, March/April 2013.

[15] N. Van Kampen, "Non-linear thermal fluctuations in a diode," *Physica*, vol. 26, pp. 585–604, August 1960.

[16] R. Menon, R. Gujarathi, A. Saffari, and J. R. Smith, "Wireless Identification and Sensing Platform Version 6.0," *ACM Conference on Embedded Networked Sensor Systems (SenSys '22)*, November 2022.

[17] MiniCircuits, "Zkl-33uln-s+ low noise amplifier." Downloaded from https://www.minicircuits.com/WebStore/dashboard.html?model=ZKL-33ULN-S%2B.

[18] RTL-SDR, "RTL-SDR Blog V3 Datasheet." Downloaded from https://www.rtl-sdr.com/wp-content/uploads/2018/02/RTL-SDR-Blog-V3-Datasheet.pdf.

[19] NESDR, "NESDR SmarteeXTR Datasheet." Downloaded from https://www.nooelec.com/store/sdr/nesdr-smartee-xtr-sdr.html.

[20] AtlasRFIDStore, "Rfmax s9028pclj." Downloaded from https://www.atlasrfidstore.com/rfmax-s9028pclj-s8658plj-lhcp-indoor-rfid-antenna-fcc-etsi/.

[21] C. A. Balanis, *Antenna Theory: Analysis and Design*. Harper & Row, Publishers, Inc., 1982.