Modulated Noise Communication: Reading UHF RFID tags without a carrier

Shanti Garman*, Ali Saffari*, Daisuke Kobuchi‡, Joshua R. Smith*†, and Zerina Kapetanovic§¶
*Department of Electrical and Computer Engineering, University of Washington, Seattle, WA, USA
†Department 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
¶Microsoft Research, Redmond, WA, USA

***Abstract*—This paper demonstrates that UHF RFID tags can be read without a carrier. More specifically, using an alternative reader design that does not emit a carrier, we show that it is possible to read an RFID tag that was designed to be read by a conventional RFID reader that does emit a carrier. Typical RFID tags are designed to modulate a carrier; it turns out that, in addition to modulating a carrier, a backscatter modulator circuit also modulates tag circuit noise, including Johnson noise; Johnson and other noise is present in a tag even if a carrier is not. Modulated Noise Communication (MNC) can be read by an alternative reader design. The reader for modulated noise communication is simpler than a conventional backscatter reader because it does not have to contend with the problem of self-jamming. The absence of a carrier means that the tag needs an alternative power source; this could be an energy harvester such as a photovoltaic cell, or could be a time-multiplexed continuous wave signal from the reader. The use of time multiplexing means that the reader would still inherit the benefits of not needing to counteract self jamming.**

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

I. Introduction

Modulated Backscatter (MBS) is a communication technique used by RFID systems, where a radio frequency (RF) signal is selectively reflected or absorbed by switching between matched and mismatched impedance states [1]. Existing RFID systems require an RFID reader to generate an RF signal source that passive wireless tags use for both energy harvesting and backscattering the RF signal to transmit information wirelessly [2], [3]. This technique allows the RFID tags to operate at very low power, have a small form factor, and operate without batteries. Similarly, researchers have demonstrated that backscatter communication techniques can be applied to ambient RF signals, such as TV and FM broadcast signals or even Wi-Fi signals. In this Ambient Backscatter communication method, a passive tag harvests energy from an ambient signal and backscatters this same signal to communicate with another nearby tag or base station [4]–[6]. These techniques have led to a wide range of RFID applications, such as tracking products in supply chains, electronic toll collection, and implantable RFID microchips for livestock. However, there are limitations to existing backscatter-based systems.

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

A challenge with existing backscatter communication systems, such as RFID, is the dependence on a generated or ambient RF source. These systems require the passive tags to be near an RFID reader or existing RF source such as a TV broadcast tower, which limits the application space. Moreover, RFID readers are expensive and involve complex hardware in order to deal with challenges such as self-jamming. Recently, researchers have demonstrated that it is possible to modulate information bits without relying on a generated RF signal [7]. Instead, the Johnson (thermal) noise in an unpowered resistor is modulated in order to transmit information bits. Specifically, the data transmitter selectively switches between connecting an antenna to an impedance-matched resistor or to an open (or short) circuit.

In this work, we show that Modulated Noise Communication (MNC) can be extended to RFID tags. We demonstrate that unmodified RFID tag hardware can wirelessly transmit information bits *without* an RF carrier; instead, it sends data by modulating noise in the RFID tag's circuitry. Although the RFID tag was designed to modulate a backscattered carrier, we show that the tag's backscattering circuitry also effectively modulates noise intrinsic to the tag, even though it was not designed for this purpose. To receive the modulated noise data, an alternative receiver (i.e., an alternative RFID reader) is required. The reader for Modulated Noise Communication does not emit a carrier and is significantly simpler than the reader for conventional modulated backscatter communication. In the remainder of this paper we present the following key contributions: **(1)** We demonstrate that a conventional RFID tag can wirelessly transmit information bits without relying on an RF carrier and **(2)** We experimentally characterize the system and evaluate performance.

II. Background on 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 [8], [9]. This thermal noise is present in any circuit element with a real impedance, regardless of whether an external voltage or current is applied. It can be characterized by its mean-squared noise voltage, which is given by,

$$v_n^2 = 4kTBR \tag{1}$$

2023 IEEE International Conference on RFID (RFID) | 979-8-3503-3551-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/RFID58307.2023.10178464

where k is Boltzmann's constant, B is bandwidth, T is temperature, and R is resistance [10]. The Johnson noise in a resistor can be modeled as a Thevenin equivalent circuit (e.g., a noiseless resistor in series with a noise voltage). Assuming an impedance-matched load is connected, the thermal noise power delivered to the load is given by,

$$P_n = \frac{v_n^2}{4R} = \frac{4kTBR}{4R} = kTB \quad (2)$$

Note that P_n is independent of resistance and is a function of temperature and bandwidth [10]. Maximum noise power transfer occurs when the Johnson noise source is impedance matched with the load circuit to which it is connected.

III. Design and Implementation

The system has two main components: a transmitter and a receiver. The data transmitter consists of standard RFID tag hardware running a custom protocol. Our implementation hardware is version 6 of the Wireless Identification and Sensing Platform (WISP 6) [11]. For this paper, the WISP 6 circuit design was not modified at all; the WISP 6 was designed to communicate with standards-compliant UHF RFID readers. To emphasize this point, even though the WISP 6 is a very new iteration of the WISP hardware, it does not contain any special features designed to support Modulated Noise Communication. Only the software running on the WISP had to be changed to implement Modulated Noise Communication. The WISP 6 has an average power consumption of $22.2\mu W$ in listening mode, and we expect that an acceleromter enabled WISP 6 tag using modulated noise communication consumes less than 396.66 μW since the data rate is lower than a regular WISP. Furthermore, we expect that earlier versions of the WISP, as well as other RFID tag hardware, should be capable of MNC data transmission, as long as the necessary protocol changes can be implemented.

The receiver uses all off-the-shelf components and follows a similar design presented in [7]. In particular, there are two Mini-Circuits ZKL-33ULN-S+ low noise amplifiers (LNAs) that provide approximately 70 dB of gain in total, followed by an RTL-SDR Blog V3 software-defined radio (SDR), and a processing unit [12], [13]. In our implementation, the processing unit is a laptop PC. Fig. 1shows the high-level hardware design, and Fig. 2A and B show the prototype implementation of the system. The hypothesis that led to this paper is that an RFID tag's backscatter modulation circuitry will typically change the impedance between its noise producing elements and its antenna, enabling Modulated Noise Communication using tag hardware that was designed for Modulated Backscatter communication.

Two primary implementations are described in this work: cabled and wireless. We first validate the proposed concept using a cabled implementation with an SMA-connectorized version of the WISP 6 board connected directly to the receive chain (see Fig. 3). The wireless implementation uses the standard WISP 6, with its standard dipole antenna, in a wireless setup transmitting to the same receive chain as the cabled experiment. The wireless implementation is the proposed approach for actually realizing RFID without a carrier. In the wireless setup, a S9028PCLJ RFID patch antenna is included at the front-end of the receive chain; this patch antenna reads the modulated thermal noise signals emitted from WISP 6's integrated dipole antenna [14].

A. Physical Principles

Johnson Noise is produced by the thermal agitation of charge carriers in dissipative (resistive) elements. The only dissipative 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, but since in the present use case the diodes are un-biased (fluctuating around zero current), their impedance is effectively constant. Unlike resistors, diodes can also exhibit shot noise, but this is only when they are carrying non-zero current; since our diodes are unbiased, Johnson Noise is expected to be the main noise source produced by the diodes.

Johnson Noise is white and broadband for frequencies $f << \frac{k_B T}{h} = 6$THz, where k_B is Boltzmann's constant, h is Planck's constant, and T=293K for room temperature. While the Modulated Noise Communication data transmitter does not contain any components actively driven at RF frequencies, the thermal noise source can be thought of as broadband and white below 6THz. However, since the WISP analog front end, WISP antenna, reader antenna, and reader low noise amplifiers are all designed for narrowband operation at 915MHz, we can focus our analysis, including impedance calculations, on 915MHz.

In the "switch closed" state, the WISP 6 used in this paper connects a 3.3 nF capacitor to ground in parallel with the rest of the WISP's analog front end, as shown in Fig 1A. In the "switch open" state, this parallel shunt capacitor is disconnected. Our hypothesis when we designed the experiments reported in this paper was that the additional low impedance pathway to ground provided by the 3.3 nF shunt capacitor (0.05 Ω at 915MHz) would decrease the observed noise. In fact, for the unmodified WISP 6 hardware, the noise level turned out to be higher in the "switch-closed" state. Investigation revealed that the particular switch used in the WISP 6 (Analog Devices ADG902 [15]) is an additional noise source that happens to produce more noise in the closed state than in the open state. Thus the sign of the noise power change was opposite of what we expected. In a further experiment, whose results are shown in Fig. 4A, we removed the switch and hardwired the WISP into each state (i.e. 3.3 nF shunt capacitor hardwired present or absent). The noise power observed in this way was consistent with our initial hypothesis: the noise power was lower with the large shunt capacitor connected. We view this as the more important result because it means that generically, the hardware of almost any backscatter tag is capable of performing modulated noise communication, without relying on less generic noise sources such as the switch noise we discovered in the WISP 6.

Despite the surprise about the sign of the noise changes, the noise power was different in the two backscatter states;

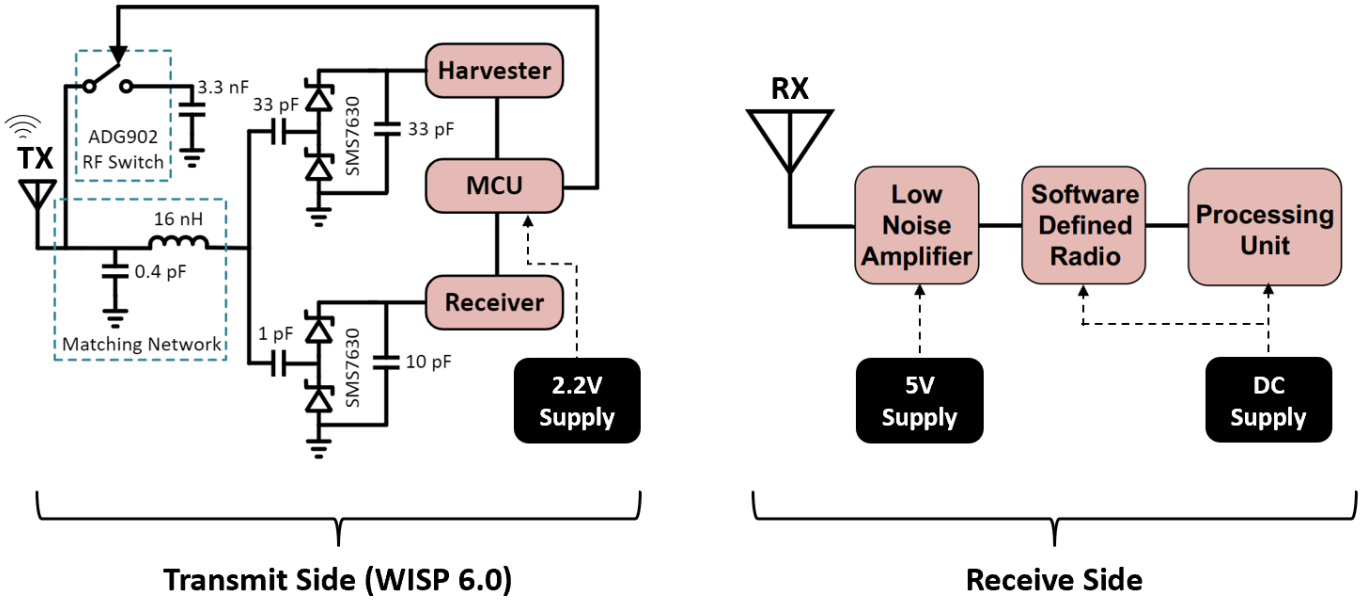


Fig. 1: **System Design.** The WISP 6 tag is used as the data transmitter. It modulates tag noise when it switches its backscatter switch between the open and closed state. The receive side includes a low noise amplifier (LNA), followed by a software-defined radio, and processing unit (e.g., laptop PC). This paper demonstrates that an RFID tag can transmit data without a carrier, simplifying the entire system architecture.

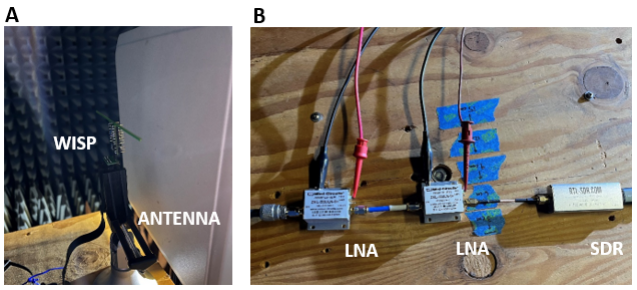


Fig. 2: **Prototype Implementation. (A)** shows the standard WISP 6 as the transmitter with a patch antenna as the receiver. **(B)** shows the remainder of the receive chain. The patch antenna output is connected to the LNA input.

as expected this enables the RFID tag to communicate using modulated noise. Because our encoding and decoding method is insensitive to the phase of the subcarrier, the error in our expectation of the sign of the noise power changes had no effect on the correctness of the data transmission and reception.

B. Data Encoding and Decoding

Similar to standard RFID tags, data is modulated by switching between two impedance states, as described above. We implement the same encoding and decoding scheme described in [7]. Data is modulated using an ON-OFF keying scheme. A 0-bit is transmitted by staying in a single state. A 1-bit is transmitted by continuously switching between the two states at a specific subcarrier frequency. In our implementation the subcarrier is set to 100 Hz. For each data transmission, we implement a packet structure that contains 20 bits. The packet begins with a 7-bit barker as the preamble, followed by a 13-bit data payload.

To receive data, the reader performs heterodyne detection at the subcarrier frequency, integrating demodulated signals into an in-phase (I) accumulator and a quadrature (Q) accumulator. Then the squared magnitude of the I and Q accumulators is computed to find the signal power at the subcarrier frequency. This demodulation method ensures that the receiver's subcarrier phase does not need to be synchronized with the data transmitter's. More detail is available in [7].

IV. Analysis and Experimental Results

Both implementations described above are evaluated in an anechoic chamber, and the results are presented in this section. First, the results of the cabled setup are presented, including the measured noise power of the system in each impedance state, as well as decoded packets from the transmission scheme. Results from the wireless setup follow. For each evaluation, the system operates at a center frequency of 915 MHz. The SDR is configured to use a sampling rate of 2 Msps; the decoding software assumes a subcarrier frequency of 100 Hz. The WISP is configured to continuously transmit data packets using a data rate of 1 bps.

A. Results from Cabled Implementation

1) Noise Power for Different Impedance States (Cabled): To validate the hypothesis that the received noise power is indeed different for the two impedance states of the WISP, noise power measurements are made with the WISP fixed in each impedance state: closed state (backscatter switch is

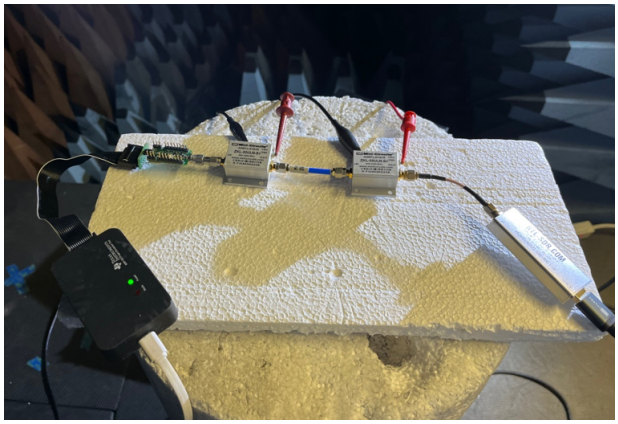


Fig. 3: **Cabled Implementation.** A SMA-connectorized version the WISP 6 tag transmits data by modulating tag noise, opening or closing a switch configured to change the impedance connected to the tag's antenna. The WISP 6 is connected directly to the receive chain via coaxial cable.

closed) and open state (backscatter switch open). For each case, all components are powered on, and raw IQ data is recorded from the SDR for a duration of 60 seconds. A Fast-Fourier Transform is performed to construct the noise power spectrum from the raw data. It was observed that the noise power when the WISP is in the closed state is larger than the noise power when the WISP is in the open state, which turned out to be because of excess noise contributed by the switch itself. Fig. 4A shows the noise differences in the two states with the excess switch noise removed. Without the switch noise, the 3.3nF state generates less noise power. A Vector Network Analyzer was also used to characterize the reflection coefficient and impedance of the two states (see Fig. 5).

2) Packet Transmission and Decoding (Cabled): Having confirmed contrast between the two impedance states suggests encoding and decoding data by modulating tag noise should be possible. To evaluate packet transmission, the WISP is set to transmit a 20-bit packet at 1 bps via Modulated Noise Communication with a 100Hz subcarrier frequency. Raw IQ data from the SDR centered at 915MHz with 1MHz sampling bandwidth (2Msps) is received, recorded, and decoded using the same encoding parameters described above. Decoded packets are shown in Fig. 4B. At the low data rate of 1 bps, packets are decoded with 100 % accuracy in the cabled setup.

B. Results from Wireless Implementation

1) Noise Power for Different Impedance States (Wireless): The same test described above is repeated, but using the wireless implementation. Results of the measured noise power spectra are shown in Fig. 6A. Similar to the cabled implementation, the wireless implementation shows a difference in noise power measured when the WISP is in the two impedance states. That said, it is also observed that the noise power when the wireless WISP is in the closed state is somewhat lower than the noise power when the SMA WISP is in the closed state, and the contrast between the two states is reduced which may impact the wireless system's ability to receive and decode packets.

2) Packet Transmission and Decoding (Wireless): With the wireless WISP positioned very close to the receive patch antenna ($d = 2$ cm), the same packet transmission is evaluated as was done with the cabled implementation described above. Decoded packets are shown in Fig. 6B. While most packets are decoded with 100 % accuracy, some evidence of non-zero bit error rate exists. This suggests that the implementation may need to be further improved in order to achieve a higher success rate on a large number of complex packets, or to support higher data rates. Ideas for such improvements are addressed in the future work section of this paper.

3) Range Experiment (Wireless): To evaluate how performance may vary with distance between the transmitter and receiver, an additional implementation is explored. Specifically, a second RFID patch antenna is connected to the SMA WISP on the transmit side. The transmit and receive patch antennas are separated by distances ranging from $d = 15$ cm to $d = 45$ cm. 15 cm is selected as the closest possible separation due to physical setup constraints. The received signal intensity is plotted in Fig. 7 and we can see that the intensity decreases as the separation distance increases.

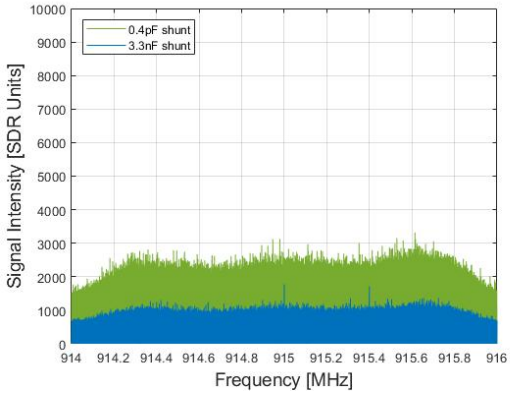
V. Future Work

While early results are promising for using standard RFID tags to communicate by MNC, there exist several areas for further investigation and optimization. Here we discuss several future research directions:

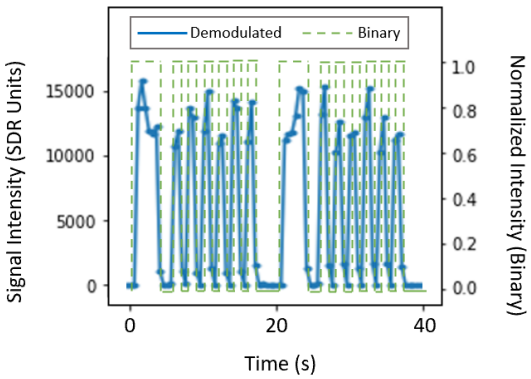
Effects due to Metallics in Proximity: Early experimental observations regarding the presence of metallic objects, such as a reflector or metal table, suggest that performance results could be improved under specific physical conditions. One hypothesis is that system performance improvements can be provided by near-field mutual impedance effects between the antenna and an external metallic object. Another hypothesis is that properly placed metals can improve the system's signal to noise ratio (more precisely, its ratio of modulated noise [signal] to un-modulated noise [noise]) by shielding the receiver from nearby sources of un-modulated thermal noise (such as the earth itself, or other nearby high emissivity materials). Additional investigations could identify potential optimizations and constraints.

RF Switch Optimization: Incorporating a different RF switch on the WISP tag could yield different results due to the different internal circuitry of the component which could affect circuit impedance values. For example, some RF switches are designed to include 50Ω shunts (e.g., ADG901) which can impact, and potentially improve the performance.

Evaluating Throughput and Communication Range: In this work, only one data rate is presented. Evaluating bit error rate (BER) and packet error rate (PER) for high volumes of complex packets at multiple data rates would provide valuable insight regarding constraints on the proposed concept. Comparing these data across cabled and wireless implementations would support further optimizations.



(a) Noise power in two impedance states



(b) Demodulated packets at 1 bps

Fig. 4: **Measured Noise Power and Demodulated Packets for Cabled Implementation. (A)** The noise power was measured from the antenna port of a WISP 6 tag (with its antenna replaced by an SMA connector). The noise power differs in the two backscatter impedance states. **(B)** Data sent by the WISP 6 via Modulated Noise Communication is demodulated successfully.

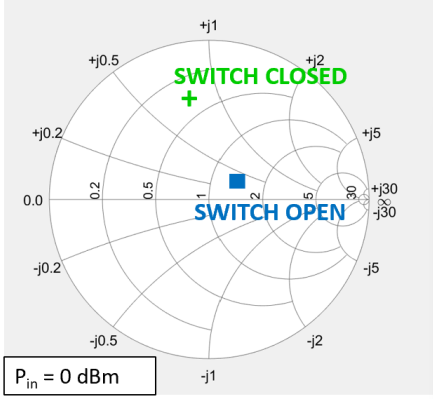


Fig. 5: **Reflection coefficient for WISP 6 in two impedance states.** The calculated reflection coefficients based on measured input impedance (S_{11}) for the two states of the WISP (switch closed and open). Measurements were made using a VNA with power of the stimulus set to 0 dBm.

Moreover, evaluating BER and PER over distance would yield valuable insights. Furthermore, evaluations should be conducted using the standard WISP antenna.

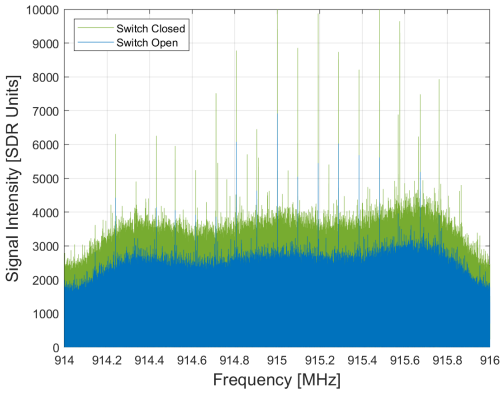
Evaluating Feedthrough: It is important to verify that there is not feedthrough from the switch control signal. This is demonstrated in [7], where communication is attempted using identical loads (which results in no detection of modulated signals). Future work to rule out feedthrough for the WISP tag in this implementation could include modifying the circuit board to create identical loads for the switch open and switch closed positions.

VI. Conclusion

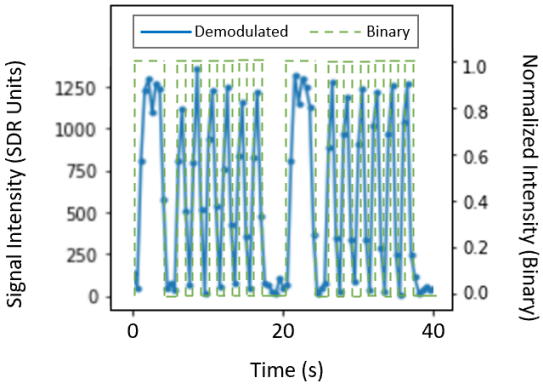
In this paper, we present promising results that indicate that it is possible to enable RFID without a carrier. Instead, wireless communication is enabled by modulating noise intrinsic to the tag. Communicating by modulating Johnson Noise is theoretically interesting from the perspective of both communication and thermodynamics.

While the WISP 6 we used for our experiments turned out to have an additional unexpected noise source (the backscatter switch itself), we expect that the hardware of almost any RFID tag should support MNC, since to implement backscatter it is necessary to modulate impedance, which will in general modulate thermal or other noise sources in the tag. It appears that a specific delicately balanced set of design parameters could prevent MNC: for example if the two impedance states produced different amounts of the thermal noise, and the two switch states also produced different amounts of noise that exactly counter-balanced the difference in thermal noise. Nevertheless, we expect that the capability to communicate data via MNC exists quite generically in backscatter hardware: designing backscatter tag hardware that is not capable of MNC would require very specific design choices.

It is difficult to predict the practical impact of this work. One can imagine designing a new type of RFID tag that relies on Modulated Noise Communication for its uplink. Such an RFID system could make use of less complex and less expensive readers, since the readers would not need to overcome self-jamming. Alternatively, a hybrid tag could be designed, that could be read by a conventional RFID reader, or an MNC reader. This work demonstrates that the un-modified analog front end of a standard RFID tag is capable of MNC; this means that MNC capabilities could be added to an existing tag design just by modifying the digital portion (or if applicable, as in the WISP) the tag's software. If one were designing a hybrid MBS / MNC RFID tag, or an MNC-only RFID tag, one would likely design the modulation circuitry differently than in the present paper, which demonstrates that a MBS tag design is capable of MNC communication. Because the range of modulated noise communication is likely to be less than that of MBS, it appears that MNC would be most appropriate for short-range applications. For example, so-called "proximity



(a) Noise power in two impedance states (wireless)



(b) Demodulated packets at 1 bps (wireless)

Fig. 6: **Measured Noise Power and Demodulated Packets for Wireless Implementation. (A)** Noise power is measured with the standard WISP tag set to two impedance states. Noise power in the two states differs, but the contrast is lower than in the cabled implementation. **(B)** Data sent wirelessly by the WISP 6 via Modulated Noise Communication is received successfully.

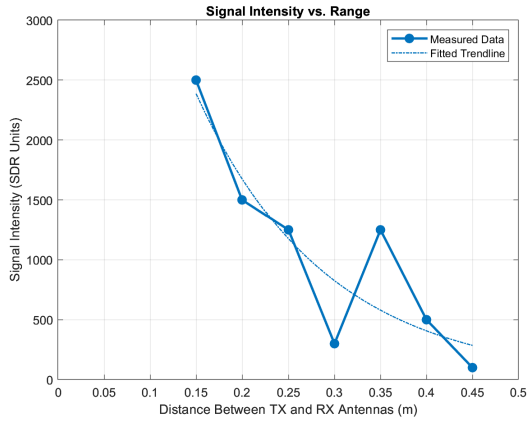


Fig. 7: **Received Intensity vs. Distances.** Received signal intensity for wirelessly transmitted data packets.

tags," such as those used in credit cards, building access cards, and metropolitan transportation systems, would seem to be likely choices.

An additional set of potential applications are implantable and wearable bio-sensors. In these applications, the lack of a carrier has an additional advantage from the perspective of RF health, since a strong carrier would not need to be directed at a patient's body. On the other hand, to achieve this benefit, a power source other than the RF carrier would be needed: our proposal to time multiplex between RF power and modulated noise communication would not have this benefit.

It is possible in some circumstances that MNC could enable new side-channel attacks on backscatter devices. Counteracting this possible attack vector would require careful designs that balance differences in thermal noise that appear to be generic to backscatter with "masking" noise sources to eliminate the noise contrast between the backscatter states. Alternatively, it might be possible to design a backscatter modulator that presents the same real impedance, and thus 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] H. Nyquist, "Thermal agitation of electric charge in conductors," *Phys. Rev.*, vol. 32, pp. 110–113, Jul 1928.

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

[10] D. M. Pozar, *Microwave Engineering*. John Wiley & Sons, Inc., 2012.

[11] 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.

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

[13] 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.

[14] A. R. Store, "Rfmax s9028pclj." Downloaded from https://www.atlasrfidstore.com/rfmax-s9028pclj-s8658plj-lhcp-indoor-rfid-antenna-fcc-etsi/?utm$_device = cutm_feeditemid = utm_term = utm_source = googleutm_medium = cpcutm_campaign = 03 - Shopping - Top$.

[15] Analog Devices, "ADG901 ADG902 Datasheet." Downloaded from https://www.analog.com/media/en/technical-documentation/data-sheets/ADG901$_902.pdf$.