Securing Inductively-Coupled Communication

Lav R. Varshney,*† Pulkit Grover,‡§ and Anant Sahai‡
*Research Laboratory of Electronics, Massachusetts Institute of Technology
†IBM Thomas J. Watson Research Center
‡Wireless Foundations, University of California, Berkeley
§Department of Electrical Engineering, Stanford University

***Abstract*—Communication over inductively-coupled links is becoming prevalent in service delivery for medical, financial, and physical security applications and so there is a growing need to prevent eavesdropping. This paper presents circuit-theoretic and communication-theoretic models of inductively-coupled communication systems. Due to coupling, the presence of an eavesdropper detunes the transfer function between the legitimate users. It is shown this detuning can be detected to reveal the presence of the eavesdropper. Further, if capacity-approaching codes are employed, neither the eavesdropper nor the legitimate receiver are able to reconstruct the transmitted message with low error probability, effectively destroying the message. Building on this insight, a coding-based secure communication protocol for inductively-coupled communication, inspired by quantum key distribution, is developed. The notion of security is defined operationally in terms of probabilities rather than through traditional notions of equivocation.**

I. Introduction

Provisioning information and energy over inductively-coupled links is becoming common in many engineering systems including medical/scientific implants [1], RFID systems [2], [3], and near-field communications systems for commerce [4], though it should be noted that inductive telegraphy was a popular means of communicating with moving trains a century ago [5, Chapter VII]. As such, there has been recent interest in information-theoretic characterization of the ultimate limits in simultaneously transmitting energy and information in the presence of noise [6], [7] as well as in the presence of timing errors [8], [9].

Separately, there has been interest in understanding the privacy and security aspects of inductively-coupled systems. With the emergence of RFID in customer-facing service delivery rather than simply back-office logistical operations [10], there is a growing business need for securing such communications. This is particularly important when transmitted information involves medical data, financial transactions, or physical access control signals. One particular kind of privacy attack is eavesdropping, where a third party antenna is used to couple into the communication channel and capture some information; the literature in this area (including a recount of effective attacks in practice) is well-summarized in [11]; one recently proposed approach to protect against eavesdroppers is active jamming [12].

Contrary to traditional studies of wireless communication that use far-field models of electromagnetics, inductive coupling is a *near-field* effect, i.e. the distance between the participating antennas is comparable to (or smaller than) the transmission wavelength. As antennas are brought to near-field, the nature of interaction changes fundamentally. Rather than the transmitting antenna remotely oscillating electrons in the receiving antenna, there is magnetic flux that induces a current from one antenna to the other through the air. Hence, unlike traditional models of wireless channels [13] where the channel between the legitimate parties is independent of the channel used by the eavesdropper, all parties are mutually coupled.

Security for inductively-coupled communication has previously been connected [14], [15] to the wiretap channel [16], a canonical problem in information-theoretic security [17]. However [14], [15] do not use a physical model for an inductively-coupled link. Ytrehus points out that for inductive coupling, "an eavesdropper needs to insert his/her own additional antenna into the system, and this may detune the overall system and make it difficult or impossible to carry out the legitimate conversation" [3].

What is *detuning*? Inductively-coupled links are tuned so that the signal is transmitted around the resonant frequency in the transfer function between the two terminals. The presence of an eavesdropper in the system could change the transfer functions, including shifting the resonant frequency, leading to detuning. The detuning effect resembles the effect of measurement in quantum mechanical systems in that it fundamentally perturbs the system; here it modifies the spectral response of the transmitted signal rather than causing waveform collapse as in quantum systems.

Building on this observation, this paper proposes a strategy to detect the presence of an eavesdropper based on spectral change. Not only can the presence of an eavesdropper be detected in quantum communication, but the desired information content of the signal is also destroyed. Can analogous information destruction be attained in our classical setting? Indeed, by using capacity-approaching codes to essentially make transmitted signals fragile, we show detuning can lead to high error probability[1] in the reconstructed signal. Taking a cue from quantum key distribution [19], this largely conceptual paper explains how one can exploit the detuning effect for

[1]Unlike traditional results in information-theoretic security [17], our notion of secrecy is defined directly in an operational way without appealing to the notion of equivocation. Shannon's notion of perfect secrecy requires the equivocation to be zero [18]; weak secrecy requires the equivocation rate to go to zero; and strong secrecy requires the (unnormalized) equivocation to go to zero. Here, the notion of secrecy is defined directly in terms of probability of unauthorized release.

secure communication using coding.

An important caveat about our assumed system model should be stated. We assume that the transmitter and receiver both know the main statistical parameters of the channel (transfer function and noise power) in the absence of the eavesdropper. These are determined primarily by

- physical geometry of the antennas (their relative positioning and the relative angles of their axes); and
- the presence of other conducting materials in the environment that are also inductively-coupled into the system.

In practical systems, obtaining knowledge of these properties precisely may be difficult. Indeed there may be several unknown conducting objects proximate to the communication system, including:

- *Bystanders* that have no particular goal, but are just nearby so as to have mutual inductance with the system. As a typical example [20]: "clusters of RFID tags in close proximity to each other, for example, exhibit significant detuning effects caused by their mutual inductances."
- *Scavengers* that are trying to harvest as much energy as possible from the legitimate transmission, treating it as ambient energy [21].
- *Jammers* that are trying to have a deleterious impact on transmission between the two legitimate terminals.

Here we ignore these possibilities to cleanly examine the potential of securing communication over inductively-coupled channels.

The remainder of the paper is organized as follows. First the near-field electromagnetic problem is converted into a circuit problem using models of mutual inductance. This allows the use of circuit theory to derive transfer functions for the inductively-coupled system, when there are just the legitimate users and when there is also an eavesdropper present. A detuning effect caused by the eavesdropper is exemplified in a particular linear geometry. Assuming the presence of additive white Gaussian thermal noise, the optimal waterfilling power allocation in the absence of the eavesdropper is derived. With the waterfilling allocation, detecting the presence of the eavesdropper is treated as a binary spectrum sensing hypothesis testing problem: probabilities of error and unauthorized release are discussed. Next, a key distribution scheme that would allow nearly secure communication is delineated. The paper closes with a discussion of future directions.

II. Circuit Model

Although inductive coupling is very much an electromagnetic field phenomenon, it behooves us to study it in terms of an equivalent circuit model [22, Ch. 1] by using differential equation relations for mutual inductance derived from Faraday's Law [23, Ch. 8].

A. Transfer Functions with Eavesdropper

Consider the communication system depicted in Fig. 1. The legitimate transfer function $V_2(j\omega)/I_1(j\omega)$ is given by

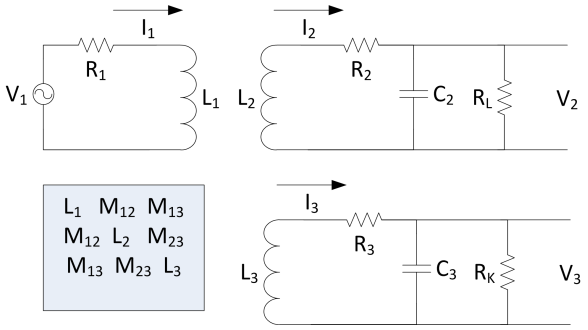

Fig. 1. A circuit model of the communication system with transmitter 1, legitimate receiver 2, and eavesdropper 3. The mutual inductance matrix among the three inductors is also indicated.

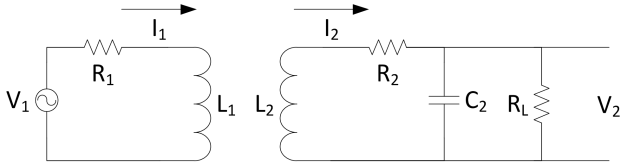

Fig. 2. A circuit model of the communication system with transmitter 1 and legitimate receiver 2.

$$\frac{V_2(j\omega)}{I_1(j\omega)} = \frac{j\omega M_{12} + \frac{(j\omega)^2 M_{12}M_{23}}{Z_K + j\omega L_3 + R_3}}{1 + \frac{R_2}{Z_L} + \frac{j\omega L_2}{Z_L} - \frac{(j\omega M_{23})^2}{(Z_K + j\omega L_3 + R_3)Z_L}}. \tag{1}$$

We relegate the derivation to Appendix A.

Analogously, the transfer function of the eavesdropper is

$$\frac{V_3(j\omega)}{I_1(j\omega)} = \frac{j\omega M_{13} + \frac{(j\omega)^2 M_{13}M_{23}}{Z_L + j\omega L_2 + R_2}}{1 + \frac{R_3}{Z_K} + \frac{j\omega L_3}{Z_K} - \frac{(j\omega M_{23})^2}{(Z_L + j\omega L_2 + R_2)Z_K}}. \tag{2}$$

B. Transfer Function without Eavesdropper

What happens when the eavesdropper is not coupled into the system, i.e. $M_{13} = M_{23} = 0$? Then the transfer function is:

$$\frac{V_2(j\omega)}{I_1(j\omega)} = \frac{j\omega M_{12}}{1 + \frac{j\omega L_2 + R_2}{Z_L}} \tag{3}$$

This can alternatively be obtained directly from the simplified circuit, Fig. 2.

So now we have current-to-voltage transfer functions for the legitimate transmission in the absence and in the presence of an eavesdropper.

C. Detuning

One might wonder how the eavesdropper affects the legitimate transfer function and in particular how the resonant frequency is detuned. Moreover, one might wonder what the eavesdropper's transfer function is when causing detuning. To indicate the general phenomenon, here we provide a series of examples in a particular geometry. Geometry is the spatial configuration of the transmitter, receiver and eavesdropper in terms of the relative placement of coils and the angles of their axes.

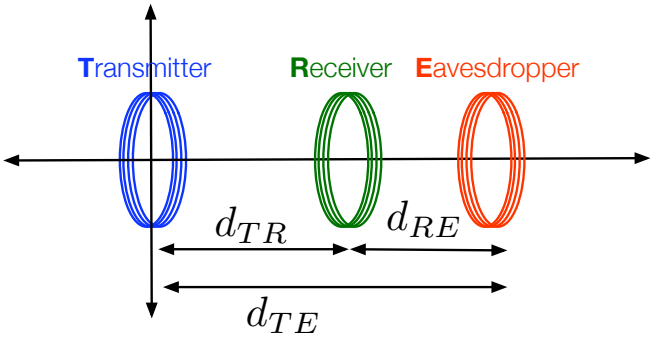

Fig. 3. Linear geometry of an inductively-coupled communication system with an eavesdropper. The distance between the several terminals are d_{RE}, d_{TR}, and d_{TE}.

Consider the linear coil geometry depicted in Fig. 3; although the eavesdropper is drawn further from the transmitter than the legitimate receiver, it can also be between the two legitimate terminals. Assuming equal number of coil turns and identical magnetic properties, by Stokes' theorem [2], the mutual inductances among the terminals are approximately governed by distances d_{TR}, d_{TE}, and d_{RE}. In particular, we use the approximations:

$$M_{ij} \approx \min\left(\sqrt{L_i L_j}, \frac{\sqrt{L_i L_j}}{d_{ij}}\right). \tag{4}$$

Exact mutual inductance expressions for this geometry and other more complicated geometries are rather complicated and their derivation is still in fact an active area of research; see [24] and references thereto. Note that the mutual inductance matrix

$$L = \begin{bmatrix} L_1 & M_{12} & M_{13} \\ M_{12} & L_2 & M_{23} \\ M_{13} & M_{23} & L_3 \end{bmatrix} \tag{5}$$

must be symmetric and positive semidefinite due to conservation of energy.

Fig. 4 shows the transfer functions of the legitimate receiver and of the eavesdropper as the eavesdropper is moved from in-between the legitimate terminals in the first panel to outside at farther and farther distances in the remaining panels. The legitimate transfer function without the eavesdropper is shown for comparison.

The detuning effect is readily apparent in these plots. In particular, when the eavesdropper is far from the legitimate terminals, the legitimate transfer function is not detuned very much and the eavesdropper has a much weaker channel transfer function. When the eavesdropper is in between or close to the legitimate terminals, the detuning effect is rather pronounced. Moreover, the eavesdropper's transfer function may be greater than the legitimate receiver's transfer function for some subset of frequencies.

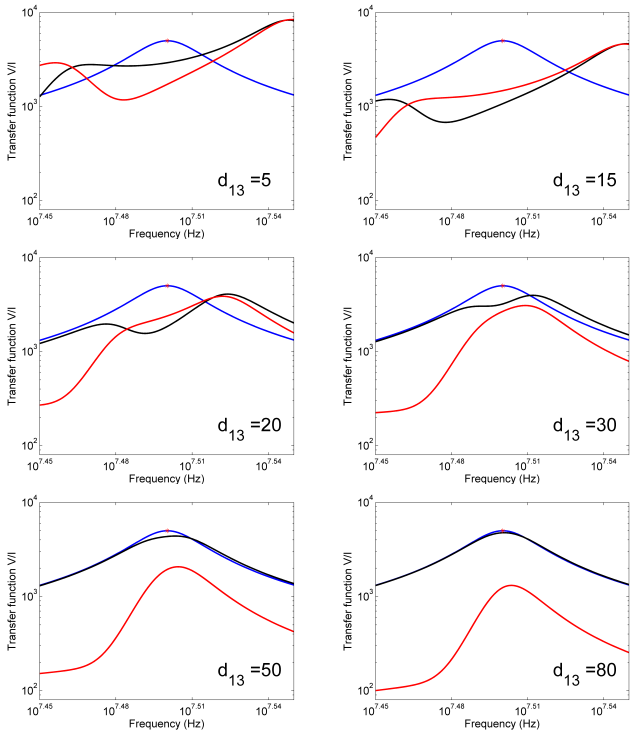

Fig. 4. Detuning with an eavesdropper coupled to the system under the linear geometry of Fig. 3. The blue line is $|V_2(f)/I_1(f)|$ for the communication system when the eavesdropper is absent and the black line is when the eavesdropper is present. The resonant frequency (without the eavesdropper) is denoted by the red star. The red line indicates the eavesdropper's transfer function $|V_3(f)/I_1(f)|$. The fixed circuit parameters are the self inductances $L_1 = 0.1$ mH, $L_2 = 0.1$ mH, and $L_3 = 0.1$ mH; the resistances $R_1 = 100$ Ω, $R_2 = 100$ Ω, and $R_3 = 100$ Ω; the load resistances $R_L = 100$ kΩ, and $R_K = 100$ kΩ; and load capacitances $C_2 = 10$ pF, and $C_3 = 10$ pF. The mutual inductances among the parties are determined from the geometry (4). The distance between the legitimate terminals is fixed at $d_{\mathrm{TR}} = 10$ m. The distance between the transmitter and eavesdropper (and thereby between the legitimate receiver and eavesdropper) is varied in the several subplots: $d_{\mathrm{TE}} = d_{13}$.

III. Communication Model

A. System model

Having developed the noiseless transfer functions in the presence and absence of an eavesdropper, now we enhance the model to include thermal noise, which is treated as additive white Gaussian noise (AWGN) at the V_2 terminal (and at the V_3 terminal). As has been previously established [7], such an inductively-coupled system is an AWGN channel with frequency-selective fading. As in [7], we assume that the transmitter and the legitimate receiver know the transfer function exactly *in the absence of the eavesdropper*, i.e. they know the terms $L_1, L_2, M_{12}, C_2, R_1, R_2, R_L$ and the thermal noise intensity. The terms $L_3, M_{13}, M_{23}, R_3, R_K, C_3$ are not known at either of the legitimate terminals.

B. Waterfilling

For a time-invariant frequency-selective channel with input x_k, output y_k, AWGN w_k with one-sided power spectral density N_0, and channel impulse response h_k, the input-output

relation is $y_k = (h \star x)(k) + w_k$, where $(h \star x)(k)$ denotes the convolution of sequences h_k and x_k evaluated at time instant k. The channel impulse response is derived from the circuit parameters which are known. We assume there is an average transmit power constraint P.

The optimal input distribution of $\{x_k\}$ required to achieve capacity is determined in part by the channel frequency response $H(f)$. For a power distribution $Q(f)$ that meets the power constraint $\int Q(f)df = P$, the capacity of the channel (in the usual sense of maximum information rate with arbitrarily small error probability) is:

$$C = \int \log\left(1 + \frac{|H(f)|^2 Q(f)}{N_0}\right) df. \tag{6}$$

The best $Q(f)$, denoted as $P(f)$, can be found using the convexity of the curve $\log(1+x)$.

The optimal power distribution follows waterfilling over frequency:

$$P(f) = \begin{cases} \frac{1}{\gamma_0} - \frac{1}{\gamma(f)}, & \gamma(f) > \gamma_0 \\ 0, & \gamma(f) < \gamma_0, \end{cases} \tag{7}$$

where $\gamma(f) = |H(f)|^2/N_0$ and γ_0 is a constant ensuring that the power constraint is met. This expression, originally derived by Shannon in the context of channels with colored noise [25], implies that greater power should be allocated to frequencies with higher SNR.

For the inductively-coupled circuit,

$$|H(f)|^2 = \frac{(2\pi f)^2 M_{12}^2}{(2\pi f)^4 K_4 + (2\pi f)^2 K_2 + K_1}, \tag{8}$$

where $K_4 = L_2^2 C_2^2$, $K_2 = C_2^2 R_2^2 + L_2^2/R_L^2 - 2L_2C_2$, and $K_1 = 1 - 2R_2/R_L + R_2^2/R_L^2$. This gives an expression for $\gamma(f)$. Let $\ominus(f) = \{\gamma(f) > \gamma_0\}$ be the active frequencies.

C. Detuning Mismatch

If the channel frequency response differs from the frequency response for which the spectral power allocation of the signaling scheme is optimized, then the mismatch may cause error rates to no longer be negligible.[2] This is particularly true for codes that operate close to the capacity of the channel in the absence of the eavesdropper, due to the strong converse part of the noisy channel coding theorem [26]. Codes operating near channel capacity are fragile.

IV. A Secure Communication Protocol

The previous two sections defined the circuit model and communication system model, while emphasizing the detuning effect. The waterfilling allocation for optimal legitimate communication was also discussed. Now we develop a way to secure inductively-coupled communication.

[2]There are various ways to approximate or bound this error rate, e.g. by using the loss in mutual information. Although a closed form expression for the loss in mutual information is omitted, it is clear how one can be derived from (1) and (8).

A. Transmitter

By varying its current, the legitimate transmitter produces a codeword from a Gaussian codebook that is described by its spectrum $X(f)$ optimized for $H(f)$ given in (8).

Due to system coupling, the transmitter is able measure the channel transfer function. It performs a binary hypothesis test to determine the presence or absence of the eavesdropper. This test is detailed when describing the legitimate receiver.

B. Legitimate Receiver

When the legitimate receiver senses the transmitted signal, it performs two operations simultaneously. First, the spectral response of the channel is measured and second, the signal is decoded using the decoder for the Gaussian codebook.

1) Spectrum Sensing: The first operation performed by the legitimate receiver is a binary hypothesis test on whether the eavesdropper is absent or present. The (waterfilling) spectral response $X(f)$ of the transmitted signal is known and identical in the two situations. The difference in the two settings is the channel frequency response. Let it be denoted $H(f)$ with eavesdropper absent and let it be denoted $G(f)$ with eavesdropper present (this is unknown to the receiver). This means the receiver is trying to differentiate between hypotheses A_0 and A_1:

$$A_0 : Y(f) = H(f)X(f) + W(f) \tag{9}$$

$$A_1 : Y(f) = G(f)X(f) + W(f), \tag{10}$$

where $W(f)$ is AWGN. Letting $\hat{A}_0$ and $\hat{A}_1$ be the receiver decisions, four outcomes of detection are possible:

- $(A_0, \hat{A}_0)$: Eavesdropper absent, declared absent: secure communication
- $(A_0, \hat{A}_1)$: Eavesdropper absent, declared present: unnecessary caution
- $(A_1, \hat{A}_0)$: Eavesdropper present, declared absent: unknown unauthorized release
- $(A_1, \hat{A}_1)$: Eavesdropper present, declared present: known unauthorized release

Since $G(f)$ is unknown, a periodogram energy detector [27] can be used.

Due to coupling (with its attendant access to electrical currents), the transmitter also can measure the channel response and also perform an equivalent binary hypothesis test. We are interested in the maximum error probabilities between the transmitter and receiver. We use the Neyman-Pearson formulation to optimally tradeoff between unnecessary caution and unknown unauthorized release of data.

2) Decoding: The receiver uses standard channel decoding. If the eavesdropper is absent and the code has rate below capacity, reliable communication is achieved by the direct part of the noisy channel coding theorem.

As observed in Fig. 4, when the eavesdropper is present the channel is detuned and the signal-to-noise ratio over the waterfilling frequencies $\ominus(f)$ may be worse than designed for. As a consequence, by the strong converse [26], error rates will be significant.

C. Eavesdropper

The eavesdropper has two goals: evading detection and reliably decoding the transmitted message. In operation, it just does one thing: standard channel decoding using the legitimate Gaussian codebook.

As observed in Fig. 4, the transfer function of the eavesdropper over the waterfilling frequencies $\ominus(f)$ may be less than the code was designed for. When this is the case, by the strong converse [26], error rates will be significant. If this is not the case, the eavesdropper would be able to decode reliably.

D. Use of Key Distribution Protocol

In what we have described so far for the $(A_1, \hat{A}_1)$ case, the legitimate users can detect an eavesdropper only after they have communicated their message. It would be much better, however, to guarantee security *ex ante* rather than *ex post*. To do so, we enhance the prior discussion by borrowing the idea of quantum key distribution from quantum cryptography [19].

In a key distribution protocol, the legitimate users do not initially use the inductively-coupled channel to transmit message themselves, but only to transmit a random sequence of symbols: a *key*. If the key is received when the eavesdropper is declared absent, then the legitimate users can safely use this key to encode messages in a one-time pad fashion [18]. On the other hand, if the key is received when the eavesdropper is declared present, then the legitimate users can simply disregard the key and try again with a new key. Since the key was random, no loss of security was incurred.

If the entropy of a received key is larger than the entropy of a message to be sent, then by Shannon's classical argument [18], perfect secrecy can be guaranteed for a second stage transmission.

E. Analysis of Errors and Unauthorized Release

The probabilities of receiving a message without error and without unauthorized release can be analyzed formally, but in this short and conceptual paper, we describe things informally.

There are several deleterious events:

- $\mathcal{E}_1$: In the $(A_0, \hat{A}_0)$ setting, the key codeword is received in error in the first stage.
- $\mathcal{E}_2$: In the $(A_0, \hat{A}_0)$ setting, the message codeword is received in error in the second stage.
- $\mathcal{E}_3$: The $(A_1, \hat{A}_0)$ setting arises in key transmission and the eavesdropper correctly decodes the transmitted key.

The events $\mathcal{E}_1$ and $\mathcal{E}_2$ relate to erroneous reception. Their probabilities can be controlled using standard arguments from the direct part of the channel coding theorem [25].

The event $\mathcal{E}_3$ relates to unauthorized release. It has two parts: missed detection of the eavesdropper by the legitimate parties and correct decoding by the eavesdropper. The first part can be controlled using the Neyman-Pearson version of energy detection [27] and depends on how $H(f)$ differs from $G(f)$ over $\ominus(f)$. The second part can be controlled using the strong converse of the channel coding theorem [26] and depends on how $H(f)$ compares to $|V_3(f)/I_1(f)|$ over $\ominus(f)$.

Note that the use of the strong converse depends on the code being close to the capacity of the channel without the eavesdropper. If the code has a large gap to capacity, then correct decoding by the eavesdropper may not be controlled appropriately.

Further note that even when the strong converse implies large probability of error at the eavesdropper, the eavesdropper may still learn something to reduce key entropy. For one-time pad results to hold, the message entropy must remain below the key entropy [18]. Detailed study of the worst-case message entropy limit remains for future work.

F. Summary

To summarize the previous two possibilities, while also introducing a new one, there is a trichotomy such that either:

1) the eavesdropper is close enough that legitimate users feel its perturbation, or
2) the eavesdropper is far enough that legitimate users do not feel its perturbation, but that its received signal is so weak that the traditional wiretap model applies [16], or
3) the eavesdropper's perturbation is undetectable and it is receiving a weak signal over $|V_3(f)/I_1(f)|$, but somehow it has reduced its thermal noise $W(f)$ so that the signal-to-noise ratio (SNR) is sufficient for unauthorized release. Reducing thermal noise requires cryogenic cooling, but then this cold spot is detectable.

Securing against this last cryogenic possibility requires heat detection equipment in addition to communication equipment. One might wonder about frequency-selective cooling with an array of eavesdropper coils, where the SNR in a relevant frequency band is increased but by decreasing the SNR in another band, the overall temperature is not changed. There is a limit to this, since the several coils are necessarily coupled to each other and therefore cause crosstalk.

We should note that for the first (and third) possibility, any proximate conducting object causes cessation of legitimate communication. This is true whether the object is actually an eavesdropper or just a bystander with no ill intent; in secure communication, protection against bystanders is necessary. This is equivalent to quantum cryptography where malicious perturbations have the same effect as benign ones [19].

The cessation of substantive communication in our scheme suggests a way to cause a denial-of-service attack. Indeed there is no way around this, either here or in quantum cryptography [19]. One method to mitigate jamming suggested in the quantum key distribution literature is the use of quantum key distribution networks, with the hope that not all network paths have been compromised. We could also construct a network.

V. Conclusion

We have suggested a secure classical communication protocol akin to quantum cryptography, by exploiting the physical properties of inductive coupling. In practical systems, there may be other third parties that are coupled into the system such as bystanders, energy scavengers, and jammers, that we

have ignored at present but should be considered in future work.

Although inductively-coupled communication systems today may use uncoded transmission or feedback-based protocols, the use of capacity-approaching codes is central to our development through the strong converse of the channel coding theorem. The use of these codes makes transmitted information just fragile enough that the presence of an eavesdropper destroys information.

Moving forward, it would be of interest to cartographically map regions of secure communication by using the geometric/magnetic properties of mutual inductance.

ACKNOWLEDGMENT

We thank Vivek K Goyal for discussions.

APPENDIX A
TRANSFER FUNCTION

For the legitimate receiver, by Kirchhoff's Voltage Law (KVL), we get:

$$V_2 = j\omega M_{12} I_1 - j\omega L_2 I_2 + j\omega M_{23} I_3 - I_2 R_2. \tag{11}$$

By Ohm's Law, we get:

$$I_2 = V_2 \left(\tfrac{1}{R_L} + j\omega C_2 \right) = V_2 / Z_L, \tag{12}$$

where $Z_L = 1/\left(\tfrac{1}{R_L} + j\omega C_2 \right)$ is the load impedance of the legitimate receiver.

For the eavesdropper, by KVL, we get:

$$V_3 = j\omega M_{13} I_1 + j\omega M_{23} I_2 - j\omega L_3 I_3 - I_3 R_3. \tag{13}$$

By Ohm's Law, we get:

$$I_3 = V_3 \left(\tfrac{1}{R_K} + j\omega C_3 \right) = V_3 / Z_K, \tag{14}$$

where $Z_K = 1/\left(\tfrac{1}{R_K} + j\omega C_3 \right)$ is the eavesdropper's load impedance.

From (13) and (14),

$$\begin{aligned} V_3 &= j\omega M_{13} I_1 + j\omega M_{23} I_2 - (j\omega L_3 + R_3) I_3 \qquad (15) \\ &= j\omega M_{13} I_1 + j\omega M_{23} I_2 - (j\omega L_3 + R_3) \frac{V_3}{Z_K} \end{aligned}$$

and so

$$V_3 \left[1 + \frac{j\omega L_3 + R_3}{Z_K} \right] = j\omega M_{13} I_1 + j\omega M_{23} I_2. \tag{16}$$

Now, using (11) and (12),

$$V_2 = j\omega M_{12} I_1 - (j\omega L_2 + R_2) \frac{V_2}{Z_L} + j\omega M_{23} I_3. \tag{17}$$

Rearranging (17),

$$\begin{aligned} V_2 \left[1 + \frac{R_2}{Z_L} + \frac{j\omega L_2}{Z_L} \right] &= j\omega M_{12} I_1 + \frac{j\omega M_{23} V_3}{Z_K} \\ &= j\omega M_{12} I_1 + \frac{\frac{j\omega M_{23}}{Z_K} \left[j\omega M_{13} I_1 + \frac{j\omega M_{23} V_2}{Z_L} \right]}{1 + \frac{j\omega L_3 + R_3}{Z_K}} \\ &= j\omega M_{12} I_1 + \frac{j\omega M_{23}}{Z_K + j\omega L_3 + R_3} \left[j\omega M_{13} I_1 + \frac{j\omega M_{23} V_2}{Z_L} \right]. \end{aligned}$$

Thus,

$$\begin{aligned} V_2 \left[1 + \frac{R_2}{Z_L} + \frac{j\omega L_2}{Z_L} - \frac{(j\omega M_{23})^2}{(Z_K + j\omega L_3 + R_3) Z_L} \right] \\ = \left(j\omega M_{12} + \frac{(j\omega)^2 M_{13} M_{23}}{Z_K + j\omega L_3 + R_3} \right) I_1, \end{aligned}$$

which yields the transfer function

$$\frac{V_2(j\omega)}{I_1(j\omega)} = \frac{j\omega M_{12} + \frac{(j\omega)^2 M_{12} M_{23}}{Z_K + j\omega L_3 + R_3}}{1 + \frac{R_2}{Z_L} + \frac{j\omega L_2}{Z_L} - \frac{(j\omega M_{23})^2}{(Z_K + j\omega L_3 + R_3) Z_L}}. \tag{18}$$

REFERENCES

[1] R. Sarpeshkar, *Ultra Low Power Bioelectronics: Fundamentals, Biomedical Applications, and Bio-inspired Systems*. Cambridge University Press, 2010.

[2] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. Chichester, UK: John Wiley & Sons, 2003.

[3] Ø. Ytrehus, "Communication on inductively coupled channels: Overview and challenges," in *Coding Theory and Applications*, ser. Lecture Notes in Computer Science, Á. Barbero, Ed. Berlin: Springer, 2008, vol. 5228, pp. 186–195.

[4] S. Ortiz, Jr., "Is near-field communication close to success?" *IEEE Computer*, vol. 39, no. 3, pp. 18–20, Mar. 2006.

[5] J. A. Fleming, *The Principles of Electric Wave Telegraphy and Telephony*. London: Longmans, Green, and Co., 1919.

[6] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. 2008 IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 1612–1616.

[7] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *Proc. 2010 IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2363–2367.

[8] Á. I. Barbero, G. D. Horler, E. Rosnes, and Ø. Ytrehus, "Modulation codes for reader-tag communication on inductively coupled channels," in *Proc. 2008 Int. Symp. Inf. Theory Appl. (ISITA 2008)*, Dec. 2008.

[9] E. Rosnes, Á. I. Barbero, and Ø. Ytrehus, "Coding for a bit-shift channel with applications to inductively coupled channels," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM 2009)*, Dec. 2009.

[10] L. S. Lee, K. D. Fiedler, and J. S. Smith, "Radio frequency identification (RFID) implementation in the service sector: A customer-facing diffusion model," *Int. J. Prod. Econ.*, vol. 112, no. 2, pp. 587–600, Apr. 2008.

[11] G. P. Hancke, "Security of proximity identification systems," University of Cambridge Computer Laboratory, Tech. Rep. UCAM-CL-TR-752, Jul. 2009.

[12] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proc. ACM Conf. SIGCOMM 2011*, Aug. 2011, pp. 2–13.

[13] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[14] J. Bringer and H. Chabanne, "On the wiretap channel induced by noisy tags," in *Security and Privacy in Ad-Hoc and Sensor Networks*, ser. Lecture Notes in Computer Science, L. Buttyán, V. Gligor, and D. Westhoff, Eds. Berlin: Springer, 2006, vol. 4357, pp. 113–120.

[15] H. Chabanne and G. Fumaroli, "Noisy cryptographic protocols for low-cost RFID tags," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3562–3566, Aug. 2006.

[16] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[17] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[18] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[19] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Jan. 2002.

[20] C. Floerkemeier and M. Lampe, "Issues with RFID usage in ubiquitous computing applications," in *Pervasive Computing*, ser. Lecture Notes in Computer Science, A. Ferscha and F. Mattern, Eds. Berlin: Springer, 2004, vol. 3001, pp. 188–193.

[21] J. A. Paradiso and T. Starner, "Energy scavenging for mobile and wireless electronics," *IEEE Pervasive Comput.*, vol. 4, no. 1, pp. 18–27, Jan.-Mar. 2005.
[22] J. R. Pierce, *An Introduction to Information Theory: Symbols, Signals and Noise*, 2nd ed. Dover, 1980.
[23] L. O. Chua, C. A. Desoer, and E. S. Kuh, *Linear and Nonlinear Circuits*. New York: McGraw-Hill Book Company, 1987.
[24] F. W. Grover, *Inductance Calculations*. New York: Van Nostrand, 1946.
[25] C. E. Shannon, "Communication in the presence of noise," *Proc. IRE*, vol. 37, no. 1, pp. 10–21, Jan. 1949.
[26] J. Wolfowitz, "Information theory for mathematicians," *Ann. Math. Stat.*, vol. 29, no. 2, pp. 351–356, Jun. 1958.
[27] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.