# Strengthening Simmon's bound on impersonation

Johannesson, Rolf; Sgarro, Andrea

*Published in:*
IEEE Transactions on Information Theory

*DOI:*
10.1109/18.86970

1991

TABLE II
IDENTIFICATION OF AN UNKNOWN FREQUENCY BY THE AR AND THE RECURSIVE FILTER METHODS

| SNR Ratio (db) | AR Freq. Est. | Recurs. Est. |
|---|---|---|
| +29 | 0.804 | 0.8004 |
| +23 | 0.815 | 0.8004 |
| +20.5 | 0.825 | 0.8005 |
| +17.0 | 0.854 | 0.8005 |
| +11 | 0.973 | 0.8006 |
| +3.0 | 1.28 | 0.794 |

seems to lie in the recursive method's use of a narrowband filter. Ill-posedness discussed at the close of Section II had not yet even entered the picture.

## V. CONCLUSION AND EXTENSIONS

We have herein taken a step toward deriving a useful information-theoretical technology from the intriguing analytic device of HK. The specific contributions of the present work include extending the HK convergence result to general filter classes, with the specific objective of justifying use of narrowband filters. Through a fixed-point structure, we have here been able to show that the HK recursions and our generalizations thereof achieve linear convergence, and can quantify the coefficient in terms of hypothesized noise and filter parameters. Computational experiments just reported give us evidence that the recursive frequency detector explored here is clearly competitive with alternative fast algorithms.

Presentation of details here would constitute a distraction, but we will mention that many pragmatic details of the frequency detector have been explored. In particular, Kedem and Yakowitz [12] have developed a rule that narrows the bandwidth as recursions progress. This has the effect of enhancing the signal-to-noise power ratio while increasing the convergence rate (to quadratic). Through such extensions, we have developed a practical way for detecting several signal frequencies simultaneously. The scheme could be implemented by parallel processors.

In another direction, we have designed a recursive filter for tracking a spread-spectrum FM signal embedded in noise. Once the filter has "locked" onto the signal, only one recursion is needed for each update, because the correlation coefficient of a data block constitutes an accurate initial starting point $r(1)$ for its successor block. Our opinion is that this capability of effectively using information from the recent past gives the recursive detector a clear-cut computational advantage over periodogram-based algorithms.

Our methodology for the detection tasks just mentioned depends strongly on the contributions of the present work. Our ambitions now are to derive distributional properties of the sampling error, and to explore a zero-crossing version of the filter which, in light of [11], may have faster convergence properties.

## ACKNOWLEDGMENT

The author gratefully acknowledges discussions and reading suggestions offered by Profs. D. Brillinger and R. Shumway. Prof. B. Kedem has been influential and supportive of the research efforts reported here.

## REFERENCES

[1] T. W. Anderson, *The Statistical Analysis of Time Series.* New York: Wiley, 1971.
[2] G. E. P. Box and G. M. Jenkins, *Time Series Analysis Forecasting and Control.* San Francisco: Holden-Day, 1970.
[3] D. R. Brillinger, *Time Series Data Analysis and Theory.* New York: Holt, Rinehart, and Winston, Inc., 1975.
[4] B. F. Chao and F. Gilbert, "Autoregressive estimation of complex eigenfrequencies in low frequency seismic spectra," *Geophys, J. R. Astro. Soc.*, vol. 63, pp. 641–659, 1980.
[5] G. Cybenko, "Fast approximation of dominant harmonics," *SIAM J. Sci. Statist. Comput.*, vol. 5, pp. 317–331, 1984.
[6] G. Goodwin and K. S. Sin, *Adaptive Filtering Prediction and Control.* Englewood Cliffs, NJ: Prentice-Hall, 1984.
[7] E. J. Hannan and B. G. Quinn, "The resolution of closely adjacent spectral lines," preprint, 1989.
[8] S. He and B. Kedem, "Higher order crossings spectral analysis of an almost periodic random sequence in noise," *IEEE Trans. Inform. Theory*, vol. 35, no. 2, pp. 360–369, Mar. 1989.
[9] M. Huzii, "On an autoregressive model fitting and discrete spectra," in *Recent Developments in Statistical Inference and Data Analysis*, L. Matusita, Ed. Amsterdam: North Holland, 1980.
[10] B. Kedem, "Spectral analysis and discrimination by zero-crossings," *Proc. IEEE*, vol. 74, pp. 1447–1493, Nov. 1986.
[11] ——, "Detection of periodicities in higher order crossings," *J. Time Series Anal.*, vol. 8, pp. 39–50, 1987.
[12] B. Kedem and S. Yakowitz, "A contribution to frequency detection," submitted to *IEEE Trans. Commun.*, 1990.
[13] B. G. Ong and L. L. Campbell, "Estimation of frequencies of sinusoids in the presence of noise," *Canad. J. Statist.*, vol. 7, pp. 11–19, 1979.
[14] H. J. Newton and M. Pagano, "A method for determining periods in time series," *J. Amer. Statist. Assoc.*, vol. 78, pp. 152–159, 1983.
[15] W. F. Pisarenko, "The retrieval of harmonics from a covariance function," *Geophys. J. R. Astr. Soc.*, vol. 33, pp. 347–366, 1973.
[16] W. H. Press, B. R. Flannery, S. A. Teukolsky, and W. T. Vettering, *Numerical Recipes (Fortran Version).* New York: Cambridge Press, 1989.
[17] M. B. Priestley, *Spectral Analysis and Time Series.* London: Academic Press, 1981.
[18] J. A. Rice and M. Rosenblatt, "On frequency estimation," *Biometrika*, vol. 75, pp. 477–484, 1988.
[19] M. K. Simon, J .K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, 3 vols. Rockville, MD: Computer Science Press, 1985.
[20] S. Yakowitz, *Computational Probability and Simulation.* Reading, MA: Addison Wesley, 1977.

# Strengthening Simmons' Bound on Impersonation

Rolf Johannesson and Andrea Sgarro

***Abstract*—Simmons' lower bound on impersonation, $P_I \geq 2^{-I(M;E)}$, where $M$ and $E$ denote the message and the encoding rule, respectively, is strengthened by maximizing over the source statistics and by allowing dependence between the message and the encoding rule.**

***Index Terms*—Authentication, impersonation, deception, perfect authentication.**

Manuscript received June 15, 1990; revised November 15, 1990. This work was presented in part at the Monte Verità Seminar, "Future Directions in Cryptography," Ascona, Switzerland, October 15–21, 1989.
R. Johannesson is with the Department of Information Theory, Lund University, Box 118, S-221 00 Lund, Sweden.
A. Sgarro is with the Departimento di Matematica e Informatica, Università di Udine, I-33100 Udine, Italy and the Dipartimento di Scienze Matematiche, Università di Trieste, I-34100 Trieste, Italy.
IEEE Log Number 9143443.

## I. Introduction

In a system for authentication developed by Simmons [1] the transmitter and receiver privately select an encoding rule $E \in \mathscr{E}$. The transmitter observes a source state $S \in \mathscr{S}$ and uses the encoding rule $E$ to determine a message $M \in \mathscr{M}$, which is sent over a (noiseless) communication channel to the receiver. (We rule out source states and encoding rules with zero probability.) A third participant, the opponent, would like to deceive the receiver into accepting a message that will misinform him about the state of the source. The opponent can choose between two quite different attacks: *impersonating* the transmitter and trying to form a valid message when in fact nothing has been sent, or waiting for a message sent by the transmitter and trying to *substitute* some other valid message. Let $P_I$ and $P_S$ denote the opponent's best-possible probability of success in an impersonation attack and in a substitution attack, respectively.

Simmons [1], also introduced $P_d$, the probability of *deception*, i.e., the probability that the opponent succeeds in defrauding the receiver by choosing optimally between an impersonation attack and a substitution attack, and showed that

$$P_d \geq \max(P_I, P_S). \tag{1}$$

In Simmons' formulation, the opponent is assumed to know all statistics for the authentication system except for probability distribution $P(e)$ for the encoding rule $E$, which is assumed to be independent of the source state $S$. One can instead adopt the assumption, as was taken in [2], that the opponent also knows $P(e)$, in which case one has

$$P_d = \max(P_I, P_S). \tag{2}$$

Simmons' formulation is a game-theoretic one in which the sender chooses $P(e)$ to minimize $P_d$. The choice of a $P(e)$ that minimizes $P_d$ could be different from that needed to minimize the probability of success (for the opponent) of either an impersonation attack or a substitution attack, which explains the inequality in (1). However, in this paper we do not need to commit ourselves to either approach.

In Section II we review Simmons' lower bound on impersonation and in Section III we give a strengthened version of it. Two examples of authentication systems and a brief discussion are given in Section IV. We conclude the paper by showing that a refinement of our argument, which removes the assumption of independence between $E$ and $S$, leads to an even stronger bound.

## II. Simmons' Bound

The opponent's best impersonation attack is to choose the message $m$ that maximizes the probability that $m$ is a valid message. Let the *authentication function* $\chi(m,e)$ be 1 if $m$ is valid message for the encoding rule $e$, and 0 otherwise, i.e., $\chi(m,e)=0$ if and only if the joint probability $P(m,e)$ is zero. Then,

$$P_I = \max_m P(m \text{ valid}), \tag{3}$$

where

$$P(m \text{ valid}) = \sum_e \chi(m,e) P(e). \tag{4}$$

Simmons [1] (see also [2] and [3], where a short proof is provided) proved that

$$P_I \geq 2^{-I(M;E)}, \tag{5}$$

($I(M;E)$ is the mutual information) with equality if and only if

a) $P(m \text{ valid})$ is independent of $m$ or, equivalently, choosing $M$ completely at random is an optimum impersonation attack

and

b) for each message $m$, $P(m|e)$ has the same value for all $e$ for which $\chi(m,e)=1$.

The bound (5) also implies the bound

$$P_d \geq 2^{-I(M;E)}, \tag{6}$$

where a) and b) are necessary but no longer sufficient conditions for equality.

We conclude this section by giving a simple proof of Simmons' bound (5). This proof, which is a variant of the one given in [3], was suggested by Körner [4] and is based on the *log-sum inequality* [5, pp. 48–49]. For arbitrary nonnegative numbers $\{a_i\}_{i=1}^n, \{b_i\}_{i=1}^n$ we have

$$\sum_i a_i \log \frac{a_i}{b_i} \geq a \log \frac{a}{b}, \tag{7}$$

(where a term in the sum with $a_i = 0$ is understood to be 0), where $a = \sum_i a_i$ and $b = \sum_i b_i$, and where equality holds if and only if $a_i b = a b_i$ for $i = 1, 2, \cdots, n$.

For each message $m$ the summation over the encoding rules in the expression for the mutual information

$$I(M;E) = \sum_m P(m) \left( \sum_e P(e|m) \log \frac{P(e|m)}{P(e)} \right) \tag{8}$$

can be restricted to all $e$ for which $\chi(m,e)=1$, since $P(e|m)=0$, if and only if $\chi(m,e)=0$. Thus (8) can equivalently be written as

$$I(M;E) = \sum_m P(m) \left( \sum_e \chi(m,e) P(e|m) \log \frac{\chi(m,e)P(e|m)}{\chi(m,e)P(e)} \right). \tag{9}$$

Defining $a_e = \chi(m,e)P(e|m)$ and $b_e = \chi(m,e)P(e)$, we obtain $a = \sum_e a_e = 1$ and $b = \sum_e b_e = P(m \text{ valid})$.

Applying (7) to the summations over the encoding rules in (9), we obtain

$$\begin{aligned} I(M;E) &\geq -\sum_m P(m) \log P(m \text{ valid}) \\ &\geq -\max_m \log P(m \text{ valid}) = -\log P_I. \end{aligned} \tag{10}$$

Observing that the conditions for equality in (10) are equivalent to a) and b) previously given completes the proof.

## III. A Tightened Lower Bound

From (4) and (3), it is clear that $P(m \text{ valid})$ and $P_I$ are independent of the source statistics, but, in general, $I(M;E)$ is not! Thus, we can minimize $I(M;E)$ over the source statistics to obtain the stronger bound

$$P_I \geq 2^{-\inf I(M;E)}, \tag{11}$$

where the infimum is taken over all source statistics that do not alter $\chi(m,e)$, i.e., do not change the set of $(m,e)$ pairs for which $P(m,e) \neq 0$. (We have to write an infimum rather than a minimum because the minimization set is topologically open.)

We have of course the corresponding tightening of the bound (6):

$$P_d \geq 2^{-\inf I(M;E)}. \tag{12}$$

## IV. Examples and Comments

In the following authentication systems, all encoding rules are selected with equal probability and independently of the source state $S$. The possible source states are $\mathscr{S}=\{H,T\}$, head and tail. Without loss of essential generality we assume that $P(\text{head}) = p \le 1/2$.

| $E$ \ $M$ | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| 00 | H | T | | |
| 01 | T | | H | |
| 10 | | H | | T |
| 11 | | | T | H. |

We have $P_I = 1/2$ and $P_S = 1-p \ge 1/2$. The probability of deception is $P_d \ge 1/2$ with equality, if and only if $p = 1/2$. Since

$$I(M;E) = H(M) - H(M|E) = 2 - h(p), \tag{13}$$

where $h(p)$ is the binary entropy function, we have equality in Simmons' bounds (5) and (6), if and only if $p=1/2$. In our bound (11), equality is obtained regardless of the source statistics! But in our bound (12), we have equality, if and only if $p=1/2$.

If we add a third bit to the label for the encoding rules, we obtain the following authentication system:

| $E$ \ $M$ | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| 000 | H | | T | |
| 001 | T | | H | |
| 010 | T | H | | |
| 011 | H | T | | |
| 100 | | T | | H |
| 101 | | H | | T |
| 110 | | | H | T |
| 111 | | | T | H. |

In this system, we have $P_I = 1/2$ and $P_S = 1/2$, and hence, $P_d = 1/2$, *independent of the source statistics.*

Since equation (13) is valid also for this system, we have equality in (5) and (6) if and only if $p = 1/2$, but in (11) and (12) equality is regardless of the source statistics! We call an authentication system *robustly optimal* against an impersonation attack if its achieves equality in (11). The systems in both examples are robustly optimal.

Analogously to Shannon's perfect secrecy, Simmons [6] has defined an authentication system to be *perfect* if all the information about the encoding rules exchanged in private, i.e., the information required to identify the selected encoding rule, is used either to conceal the source state or else to confound the opponent. The system of the first example is perfect if and only if $p = 1/2$, but the second is never perfect.

We conclude this section by proving a consequence of (11) [1]. In an authentication system with deterministic encoding (i.e., one in which the source state $S$ and encoding rule $E$ uniquely determine the message $M$) we have

$$\begin{aligned} I(M;E) &= H(M) - H(M|E) \\ &= H(M) - H(S) \\ &\le \log|\mathscr{M}| - H(S), \end{aligned} \tag{14}$$

where $|\cdot|$ denotes the cardinality of the set. Because the right side of inequality (14) is minimized by choosing the source states equiprobably, it follows that

$$\inf I(M;E) \le \log|\mathscr{M}| - \log|\mathscr{S}| \tag{15}$$

always holds, from which Simmons' combinatorial lower bound on impersonation, $P_I \ge |\mathscr{S}|/|\mathscr{M}|$, follows by substituting (15) into (11).

## V. Further Strengthening of the Bound

From (3) and (4), it is clear that $P_I$ depends only on the (marginal) distribution of the encoding rule $E$ and on the authentication function $\chi(m,e)$. Thus, given that these are kept fixed both the source statistics and any correlation between the source state $S$ and the encoding rule $E$ are totally irrelevant. From a practical point of view an authentication system with correlated source state $S$ and encoding rule $E$ might seem farfetched. But nevertheless, since Simmons' bound (5) is valid also in this case, we have the following strengthened bound:

$$P_I \ge 2^{-\inf I(M;E)}, \tag{16}$$

where the infimum is taken over all (possibly dependent) random couples $(S,E)$ such that:

a) $E$ has the same marginal distribution as for the given system

and

b) the resulting $\chi(m,e)$ is the same as for the given system.

The following examples show that the bound (16) can return values that are strictly better than those obtained by the bound (11). We assume that the encoding rule $E$ is determined by a fair coin:

| $E$ \ $M$ | 0 | 1 | 2 |
|---|---|---|---|
| H | H | T | |
| T | T | | H. |

Let $P(S=H)=p$. Then we have $I(M;E) = H(M) - H(M|E) = H(M) - h(p)$. If $S$ and $E$ are independent, then we have $H(M) = 1 + \frac{1}{2}h(p)$, and, hence, the minimizing $P(s)$ for our bound (11) is $p = 1/2$, which gives $P_I \ge 1/\sqrt{2}$.

Now assume that $S$ and $E$ are equal with probability close to 1. Then the message $M$ is almost always 0 and both $H(M)$ and $H(M|E)$ are close to 0. The bound (16) returns the true value $P_I = 1$ for the original system where $S$ and $E$ are independent.

In order to obtain a nondegenerate ($P_I < 1$) authentication code, we modify the preceding example:

| $E$ \ $M$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | H | T | | | |
| 1 | T | | H | | |
| 2 | | | | T | H. |

The encoding rule is determined by a random experiment with $P(E=0) = P(E=1) = 1/4$ and $P(E=2) = 1/2$. As before, we let $P(S=H)=p$ and have $I(M;E) = H(M) - h(p)$. If $S$ and $E$ are independent, then we have $H(M) = \frac{3}{2} + \frac{3}{4}h(p)$, and hence, $I(M;E) = \frac{3}{2} - \frac{1}{4}h(p)$. Our bound (11) becomes $P_I \ge 2^{-5/4} \approx 0.42$. Again bound (16) is tight, which is seen from the fact that the choices $P(S=H|E=0) = P(S=T|E=1) \approx 1$ and $P(S=H|E=2) = 1/2$ return the true value $P_I = 1/2$ for the original system where $S$ and $E$ are independent.

It should be noted that the probability distribution for the source states is hardly visible in bound (16) as previously stated; actually one can take the infimum directly with respect to random couples $(M, E)$ rather than $(S, E)$.

ACKNOWLEDGMENT

The authors' debt to Gus Simmons is both obvious and gratefully acknowledged. The authors have benefited a lot from elucidatory discussions on authentication with J. Körner, J. Massey, G. Simmons, and B. Smeets.

REFERENCES

[1] G. J. Simmons, "Authentication theory/coding theory," in *Advances in Cryptology, Proc. CRYPTO 84, Lecture Notes in Computer Science, No. 196*. G. R. Blakley and D. Chaum, Eds. New York: Springer, 1985, pp. 411–431.
[2] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, 1988, pp. 533–549.
[3] A. Sgarro, "Informational divergence bounds for authentication codes," presented at *Advances in Cryptology — Eurocrypt '89*, Houthalen, April 10–13, 1989; in *Lecture Notes in Computer Science*, vol. 434, 1990, 93–101.
[4] J. Körner, private communication.
[5] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic Press, 1981.
[6] G. J. Simmons, private communication, Oct. 16, 1989.

# Two-Dimensional Harmonic Retrieval and Its Time-Domain Analysis Technique

Xian-Da Zhang

***Abstract* —We focus on 2-D harmonic retrieval. It is shown that a 2-D ARMA process is the appropriate model of 2-D sinusoids in white noise. A time-domain analysis technique is presented for resolving several closely spaced 2-D sinusoids in white noise.**

***Index Terms* —Harmonic retrieval, two-dimensional ARMA modeling, signal detection.**

## I. INTRODUCTION

The 2-D harmonic retrieval is a classic problem in multidimensional signal processing, and receives increasing interest in various fields such as sonar, radar, geophysics, etc. Up to now, all presented solutions to the problem have been based on high resolution 2-D spectral estimations including the 2-D MEM [1]–[5], linear prediction [6]–[8], ARMA model [9]–[11], and Pisarenko's generalization [3].

In this correspondence, we focus on the 2-D harmonic retrieval from a new standpoint that is different from the previous spectrum analysis techniques. The first goal of this correspondence is to show in theory that 2-D sinusoidal frequencies $(f_{1i}, f_{2i})$ are determined by $A(z_1, z_2) = 0$, where $A(z_1, z_2)$ is a 2-D characteristic polynomial consisting of AR coefficients of a 2-D ARMA model. Our second goal is to present a time domain analysis technique in order to overcome the difficulty arising when solving $A(z_1, z_2) = 0$ for $(f_{1i}, f_{2i})$.

Manuscript received October 4, 1989; revised July 12, 1990.
The author is with the Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, CA 92093, on leave from the Changcheng Institute of Meterology & Measurement (CIMM), P.O. Box 1066, Beijing 100095, China.
IEEE Log Number 9143444.

## II. PRELIMINARIES

Consider a 2-D random field $\{x(n_1, n_2)\}$ of sinusoids in additive noise $w(n_1, n_2)$ with zero-mean and variance $\sigma^2$:

$$x(n_1, n_2) = \sum_{i=1}^{M} A_i \sin(2\pi f_{i1} n_1 + 2\pi f_{i2} n_2 + \theta_i) + w(n_1, n_2), \tag{1}$$

where $A_i$ and $\theta_i$ are the amplitude and phase of the $i$th sinusoid, respectively.

Assume that the $A_i$ are deterministic and the $\theta_i$ are uniformly distributed, mutually independent, and independent of $w(n_1, n_2)$. Then it is easy to show that $x(n_1, n_2)$ is wide-sense homogeneous and its autocorrelation function is given by

$$r(l, k) = \sum_{i=1}^{M} 0.5 A_i^2 \cos(2\pi f_{i1} l + 2\pi f_{i2} k) + \sigma^2 \delta(l, k). \tag{2}$$

It is worthwhile to point out that (2) reduces to (3) for $k \equiv 0$ and to (4) for $l \equiv 0$:

$$r(l, 0) = \sum_{i=1}^{M_1} 0.5 A_i^2(f_1) \cos(2\pi f_{1i} l) + \sigma^2 \delta(l) \tag{3}$$

and

$$r(0, k) = \sum_{i=1}^{M_2} 0.5 A_i^2(f_2) \cos(2\pi f_{2i} k) + \sigma^2 \delta(k), \tag{4}$$

in which $f_{1i}$ $(i = 1, \cdots, M_1)$ and $f_{2j}$ $(j = 1, \cdots, M_2)$ represent the distinct $f_1$ and $f_2$ frequencies, respectively, and $A_i(f_1)$ and $A_j(f_2)$ are the amplitudes of sinusoids associated with these frequencies. Note that when some frequencies (say in the set of $f_{i1}$) overlap, $A_i(f_1)$ and $A_i$ will be different. For instance, if $x(n_1, n_2)$ is given by

$$x(n_1, n_2) = \sin(0.2\pi n_1 + 0.4\pi n_2) + 2\sin(0.2\pi n_1 + 0.66\pi n_2) + w(n_1, n_1),$$

where $\sigma^2 = 1$, then

$$r(l, k) = 0.5\cos(0.2\pi l + 0.4\pi k) + 2\cos(0.2\pi l + 0.66\pi k) + \sigma(l, k),$$

but,

$$r(l, 0) = 2.5\cos(0.2\pi l) + \delta(l),$$
$$r(0, k) = 0.5\cos(0.4\pi k) + 2\cos(0.66\pi k) + \delta(k).$$

Looking carefully at (3) and (4), we see that the frequencies can be determined using only the autocorrelations $\{r(l, 0)\}$, while the determination of the $f_{2j}$ requires only the use of $\{r(0, k)\}$.

## III. HARMONIC RETRIEVAL AND ITS ANALYSIS TECHNIQUE

In this section we analyze the 2-D harmonic retrieval problem in theory, and discuss how to resolve 2-D sinusoids in white noise. To make the correspondence self-contained, we briefly state the estimation of AR parameters of a 2-D ARMA model.