MUSIC and the Sharing of a Secret

Alfred M. Bruckstein

Information Systems Laboratory
Stanford University
Stanford, CA 94305

ABSTRACT

MUSIC is an algorithm developed by R. Schmidt for multitarget direction-finding from data gathered by a passive sensor array. This short note indicates how the setup of multitarget detection may be used in devising a method to distribute a secret among N trustees so that it can be recovered if and only if more than K of them agree to cooperate.

1. INTRODUCTION

The problem of designing so called "K-out-of-N secret sharing systems" has been addressed by several researchers, see for example [1]. Such a system may be useful in many cases in which a crucial decision (like opening a safe, signing an important contract or launching an all-out nuclear attack) is to be made by at least $K+1$ out of N authorized persons. A problem that preoccupies the signal processing community for quite a while already is the design of multitarget detection and tracking algorithms that efficiently use data from an array of sensors. In this framework, Ralph Schmidt [2], developed a method of multiple direction finding, based on a plausible model for the received signals and exploiting the resulting data covariance eigenstructure. His method however fails when more sources than sensors are present. It is precisely this failure that we transform into the success of our new secret sharing system.

2. DIRECTION FINDING WITH MUSIC

The model assumed for the signals received by the N sensors is the following

$$\begin{bmatrix} r_1(t) \\ r_2(t) \\ \\ r_N(t) \end{bmatrix} = \begin{bmatrix} | & | & & | \\ A(\vartheta_1) & A(\vartheta_2) & \cdots & A(\vartheta_K) \\ | & | & & | \end{bmatrix} \begin{bmatrix} s_1(t) \\ s_2(t) \\ \\ s_K(t) \end{bmatrix} + \begin{bmatrix} n_1(t) \\ n_2(t) \\ \\ n_N(t) \end{bmatrix} \quad (1)$$

where

1) $r_i(t)$ is the signal received at the i-th sensor

2) $s_j(t)$ is the signal generated by the j-th source

3) $A(\vartheta)$ is the "signature" of any source at the direction ϑ

4) n_i is an independent noise affecting the i-th sensor

In the above model the crucial assumption is that signals coming from a certain direction have a specific "signature" in the received signal and that the sensors simply add the signatures of the existing sources with the corresponding weights. The parametrized set of signature vectors, $\{A(\vartheta)\}_{\vartheta\in\Theta}$, where Θ is the parameter set - usually $[0,2\pi]$ - is appropriately called the "array manifold" since it characterizes the directional properties of the sensor array. It is usually assumed that it has the following property: for any set of parameters ϑ with less than N elements, the array manifold vectors are linearly independent. This assumption is trivially satisfied by linear sensor arrays for which the array manifold has Vandermonde-type columns, see [3]. From eq. (1) which is rewritten more compactly as

$$r(t) = A[\vartheta_i \mid i = 1,2,\ldots K]\, s(t) + n(t)$$

it is readily seen that the covariance of $r(t)$ is given by

$$R = A[\vartheta_i \mid i = 1,2,\ldots K]\, S\, A[\vartheta_i \mid i = 1,2,\ldots K]^* + N \quad (2)$$

where S is the covariance of the sources and N the noise second-order statistics. The noise is usually assumed spatially and temporally uncorrelated with a known intensity, i.e. $N = \sigma I$. The MUSIC algorithm [2],[3] exploits the above structure of the received signals' covariance. It is obvious that if $K<N$ and S is positive definite, then the matrix $R-\sigma I$ will have rank K and therefore it has a nullspace **NS** of dimension $N-K$. It is also clear that all columns of $A[\vartheta_i \mid i = 1,2,\ldots K]$ will be orthogonal to this nullspace, and thus we have the following way to determine the directions:

> For all $\vartheta\in\Theta$ compute the sum of the inner products between $A(\vartheta)$ and a basis of **NS**, for example the $N-K$ eigenvectors E_j corresponding to the zero eigenvalue of $R-\sigma I$ of multiplicity $N-K$:
>
> $$D(\vartheta) = \sum_{j=1}^{N-K} A(\vartheta)^* E_j \quad (3)$$
>
> The K points at which $D(\vartheta)$ is "almost" zero are the directions of the sources.

The "almost" in the previous sentence is there because, of course we cannot determine R exactly from the

This work was supported in part by the U. S. Army Research Office, under Contract DAAG29-79-C-0215 and by the National Science Foundation, under Grant ECS78-10003.

CH1939-8/83/0000/0225$01.00©1984 IEEE

observations. We assume however that we gathered enough received data vectors while the sources were stationary (both not moving in space and producing a statistically stationary signal) so that we can obtain good approximations of the true R.

Note also that the MUSIC procedure fails when $K = N$ since no search-enabling nullspace is available. All matrices involved have full rank, and that's all that can be said. Direction finders are in this case totally confused as all hope for the determination of the source locations is lost. This however is quite wonderful for

3. K-OUT-OF-N SECRET SHARING

Suppose we wish to hide a secret that consists of say a binary string of length mK. First we divide the sequence in K subsequences and add to the beginning of each a code of length say q determining its order among the subsequences.

Consider the resulting K subsequences as the most significant bits of K numbers $\vartheta_i|_{i=1,2,\ldots,K}$ between zero and one and decide on a parametrized "coding manifold" $A(\vartheta)$ of dimension N having all the properties of an array manifold. For example, we may simply choose $A(\vartheta)^* = [1\ \vartheta\ \vartheta^2\ \ldots\ \vartheta^N]$.

Now generate a sequence of i.i.d. Gaussian random vectors s of dimension K according to some randomly chosen covariance structure S, and perhaps also a Gaussian noise sequence n, and produce N sequences of numbers corresponding to the entries of the received vectors r in (1). Distributing those sequences among N people will have the effect of dividing the secret among them in such a way that it is imperative for more than K of them to cooperate in order to recover it.

Indeed, if $K+1$ or more trustees decide to obtain the secret then they can use the MUSIC algorithm to direct a search on the (properly quantized) parameter space. Since only an approximation of the second order statistics R can be obtained, the parameters ϑ will be recoverable only up to a certain accuracy. However we can make the data sequences long enough so that their first $m+q$ bits will not be affected and then the decoding will be completely successful. If however only K of them decide to cooperate they have absolutely no way of determining the secret since any assumed set of values for the hidden parameters is equally valid in explaining the second order structure of the data.

This is obvious since in the case of $N = K$ we may choose an arbitrary set of parameters $\eta_i|_{i=1,2,\ldots,K}$ and those will provide the following estimate of S:

$$A_K^{-1}[\eta_i|_{i=1,2,\ldots,K}](R_K-\sigma I)A_K^{*-1}[\eta_i|_{i=1,2,\ldots,K}] = S_K' \qquad (4)$$

Thus the estimate for the second order statistics of the coding noises that would correspond to any assumed secret is a valid positive definite covariance matrix. But, by assumption, the people sharing the secret have no information on the true S, apart from the fact that it is positive definite. Hence, from the data available K (or less) conspirators will not be able to determine the secret.

Note that in the above development we assumed that for any consistent choice of say J elements of the $A(\vartheta)$ vectors we obtain a valid sub-array manifold $\{A_J(\vartheta)\}_{\vartheta\in\Theta}$ and, again, Vandermonde-type vectors will do. Also the trustees need to know what was their ordering when receiving the data strings, i.e. to know which of the r_i sequence they got.

Some further thought about the above procedure reveals that what we have in fact done is to distribute information on the matrix $R-\sigma I$ among N persons in such a way that when any group meets they know the corresponding submatrix completely, without being able to recover any other elements of it. We can, however, devise a completely deterministic scheme that achieves the same thing: just give the i-th person the second half of the bits of r_{ij} for $j<i$, the full number of bits of r_{ii} and the first half of the bits of r_{ij} for $j>i$. This method clearly meets the objective, and there are probably many others.

As before, concerning the security of this secret sharing scheme we can say the following: when more than K persons cooperate they can fully recover the parameters ϑ_i, whereas cooperation among K or less of them leaves complete uncertainity about the secret, since according to (4) any assumed set of parameters provides a valid explanation of the data. From the point of view of number of degrees of freedom it is clear that in ASA^* we have chosen $K + K(K+1)/2$ parameters, and in order to be able to recover all of them we need a submatrix of $R-\sigma I$ with dimension of at least $K + 1$, providing $(K+1)(K+2)/2 = K + K(K+1)/2 + 1$ independent parameters.

4. CONCLUDING REMARKS

We presented a new system of sharing a secret among N trustees so that it is required that more than K of them wish to cooperate in order to gain access to it. The method exploits the failure of direction finding algorithms to resolve the directions of radiating sources when their number exceeds the number of available sensors. We did not address here the issue of an information theoretic proof for the security of the system since we have an argument showing that with a submatrix of dimension $K\times K$ or less *all* possible messages can adequately explain the data.

We note that this new secret sharing system clearly has a finite field counterpart, however we did not pursue this point. It is also worth pointing out that the new method differs significantly from previous approaches, see [1] and [4]. The solution to the secret sharing problem discussed by Karnin, Greene and Hellman forms a vector in which the secret is embedded and then multiplies it by a matrix that has some "array manifold" properties. Our system uses a complementary approach, in which the secret is embedded in the array manifold matrix instead. It would perhaps be worthwhile to further analyze those two methods comparatively.

5. REFERENCES

[1] Shamir, A., "How to Share a Secret", Com. of ACM, Vol 22/11, November 1979

[2] Schmidt, R.O., "Multiple Emitter Location and Signal Parameter Estimation" Proceedings RADC Spectrum Estimation Workshop, October 1979

[3] Schmidt, R.O., "A Signal Subspace Approach to Multiple Emitter Location and Spectral Estimation", PhD Thesis, Stanford University, Stanford, November 1981

[4] Karnin, E.D., Greene, J.W. and Hellman M.E., "On Secret Sharing Systems" IEEE Trans. IT-29/1, January 1983