On Communication over Gaussian Sensor Networks with Adversaries: Further Results

Emrah Akyol[1], Kenneth Rose[1], and Tamer Başar[2]

[1] University of California, Santa Barbara
{eakyol,rose}@ece.ucsb.edu
[2] University of Illinois, Urbana-Champaign
basar1@illinois.edu

Abstract. This paper presents new results on the game theoretical analysis of optimal communications strategies over a sensor network model. Our model involves one single Gaussian source observed by many sensors, subject to additive independent Gaussian observation noise. Sensors communicate with the receiver over an additive Gaussian multiple access channel. The aim of the receiver is to reconstruct the underlying source with minimum mean squared error. The scenario of interest here is one where some of the sensors act as adversary (jammer): they aim to maximize distortion. While our recent prior work solved the case where either all or none of the sensors coordinate (use randomized strategies), the focus of this work is the setting where only a subset of the transmitter and/or jammer sensors can coordinate. We show that the solution crucially depends on the ratio of the number of transmitter sensors that can coordinate to the ones that cannot. If this ratio is larger than a fixed threshold determined by the network settings (transmit and jamming power, channel noise and sensor observation noise), then the problem is a zero-sum game and admits a saddle point solution where transmitters with coordination capabilities use randomized linear encoding while the rest of the transmitter sensors is not used at all. Adversarial sensors that can coordinate generate identical Gaussian noise while other adversaries generate independent Gaussian noise. Otherwise (if that ratio is smaller than the threshold), the problem becomes a Stackelberg game where the leader (all transmitter sensors) uses fixed (non-randomized) linear encoding while the follower (all adversarial sensors) uses fixed linear encoding with the opposite sign.

Keywords: Game theory, sensor networks, source-channel coding, coordination.

1 Introduction

Communications over sensors networks is an active research area offering a rich set of problems of theoretical and practical significance, see e.g., [8] and the

S.K. Das, C. Nita-Rotaru, and M. Kantarcioglu (Eds.): GameSec 2013, LNCS 8252, pp. 1–9, 2013.

references therein. Game theoretic considerations, i.e., the presence of adversary and its impact on the design of optimal communication strategies have been studied for a long time [9,10]. In this paper, we extend our prior work on the game theoretic analysis of Gaussian sensor networks, on a particular model introduced in [7], by utilizing the results on the game theoretic analysis of the Gaussian test channel in [3–6].

In this paper, we consider the sensor network model illustrated in Figure 1 and explained in detail in Section 2. The first M sensors (i.e., the transmitters) and the receiver constitute Player 1 (minimizer) and the remaining K sensors (i.e., the adversaries) constitute Player 2 (maximizer). This zero-sum game does not admit a saddle-point in pure strategies (fixed encoding functions), but admits one in mixed strategies (randomized functions).

Our prior work considered two extremal settings [2], depending on the "coordination" capabilities of the sensors. Coordination here refers to the ability of using randomized encoders, i.e., all transmitter sensors and the receiver; and also the adversaries among themselves agree on some (pseudo)random sequence, denoted as $\{\gamma\}$ (for transmitters and the receiver) and $\{\theta\}$ (for adversaries) in the paper. The main message of our prior work is that "coordination" plays a pivotal role in the analysis and the implementation of optimal strategies for both the transmitter and adversarial sensors. Depending on the coordination capabilities of the the transmitters and the adversaries, we considered two extreme settings. In the first setting, we considered the more general case of mixed strategies and present the saddle-point solution in Theorem 1. In the second setting, encoding functions of transmitters are limited to the fixed mappings. This setting can be viewed as a Stackelberg game where Player 1 is the leader, restricted to pure strategies, and Player 2 is the follower, who observes Player 1's choice of pure strategies and plays accordingly.

In this paper, we consider a more practical setting where only a given subset of the transmitters and also the adversarial sensors can coordinate. Our main result is: if the number of transmitter sensors that can coordinate is large enough compared to ones that cannot, then the problem becomes a zero-sum game with a saddle point, where the coordination capable transmitters use randomized linear strategy and incapable transmitters are not used at all. Discarding these transmitter sensors is rather surprising but the gain from coordination compansates for this loss. Coordination is also important for the adversarial sensors. When transmitters coordinate, adversaries must also coordinate to generate identical realizations of Gaussian jamming noise. In contrast with transmitters, the adversarial sensors which cannot coordinate is of use: they generate independent copies of the identically distributed Gaussian jamming noise. Otherwise, i.e., the number of coordinating transmitters are not large enough, transmitters use deterministic (pure strategies) linear encoding, i.e., $g_T(X) = \alpha_T X$ and optimal adversarial strategy is also uncoded communications in the opposite direction of the transmitters, i.e., $g_A(X) = \alpha_A X$ for some $\alpha_T, \alpha_A \in \mathbb{R}^+$. For both settings, uncoded communication is optimal and separate source and channel coding is strictly suboptimal.

This paper is organized as follows. In Section 2, we present the problem definition. We review prior work, particularly [2] in Section 3. In Section 4, we present our main result and finally we provide conclusions in Section 5.

2 Problem Definition

In general, lowercase letters (e.g., x) denote scalars, boldface lowercase (e.g., $\boldsymbol{x}$) vectors, uppercase (e.g., U, X) matrices and random variables, and boldface uppercase (e.g., $\boldsymbol{X}$) random vectors. $\mathbb{E}(\cdot)$, $\mathbb{P}(\cdot)$ and $\mathbb{R}$ denote the expectation and probability operators, and the set of real numbers respectively. $Bern(p)$ denotes the Bernoulli random variable, taking values 1 with probability p and -1 with $1-p$. Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance matrix R is denoted as $\mathcal{N}(\boldsymbol{\mu}, R)$.

The sensor network model is illustrated in Figure 1. The underlying source $\{S(i)\}$ is a sequence of i.i.d. real valued Gaussian random variables with zero mean and variance σ_S^2. Sensor $m \in [1 : M+K]$ observes a sequence $\{U_m(i)\}$ defined as

$$U_m(i) = S(i) + W_m(i), \tag{1}$$

where $\{W_m(i)\}$ is a sequence of i.i.d. Gaussian random variables with zero mean and variance $\sigma_{W_m}^2$, independent of $\{S(i)\}$. Sensor $m \in [1 : M+K]$ can apply arbitrary Borel measurable function $g_m^N : \mathbb{R}^N \to \mathbb{R}$ to the observation sequence of length N, $\boldsymbol{U}_m$ so as to generate sequence of channel inputs $X_m(i) = g_m^N(\boldsymbol{U}_m)$ under power constraint:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \mathbb{E}\{X_m^2(i)\} \leq P_m \tag{2}$$

The channel output is then given as

$$Y(i) = Z(i) + \sum_{j=1}^{M+K} X_j(i) \tag{3}$$

where $\{Z(i)\}$ is a sequence of i.i.d. Gaussian random variables of zero mean and variance σ_Z^2, independent of $\{S(i)\}$ and $\{W_m(i)\}$. The receiver applies a Borel measurable function $h^N : \mathbb{R}^N \to \mathbb{R}$ to the received sequence $\{Y(i)\}$ to minimize the cost, which is measured as mean squared error (MSE) between the underlying source S and the estimate at the receiver $\hat{S}$ as

$$J(g_m^N(\cdot), h^N(\cdot)) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \mathbb{E}\{(S(i) - \hat{S}(i))^2\} \tag{4}$$

for $m = 1, 2, \ldots, M+K$.

The transmitters $g_m^N(\cdot)$ for $m \in [1:M]$ and the receiver $h^N(\cdot)$ seek to minimize the cost (4) while the adversaries aim to maximize (4) by properly choosing $g_k^N(\cdot)$

for $k \in [M+1:M+K]$. We focus on the symmetric sensor and symmetric source where $P_m = P_T$ and $\sigma^2_{W m} = \sigma^2_{W T}$, $\forall m \in [1:M]$ and $\sigma^2_{W_k} = \sigma^2_{W_T}$ and $P_k = P_A$, $\forall k \in [M+1:M+K]$.

A transmitter-receiver-adversarial policy $(g_m^{N*}, g_k^{N*}, h^{N*})$ constitutes a saddle-point solution if it satisfies the pair of inequalities

$$J(g_m^{N*}, g_k^{N}, h^N) \leq J(g_m^{N*}, g_k^{N*}, h^{N*}) \leq J(g_m^{N}, g_k^{N*}, h^N) \tag{5}$$

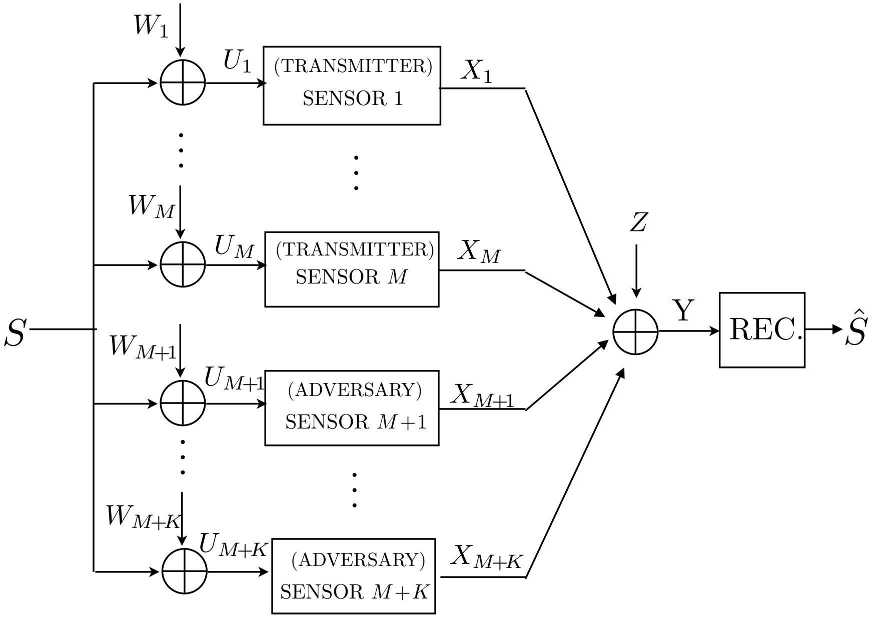

Fig. 1. The sensor network model

3 Review of Prior Work

3.1 Full Coordination

First scenario is concerned with the setting where "all" transmitter sensors have the ability to *coordinate*, i.e., all transmitters and the receiver can agree on an i.i.d. sequence of random variables $\{\gamma(i)\}$ generated, for example, by a side channel, the output of which is, however, not available to the adversarial sensors[1]. The ability of coordination allows transmitters and the receiver to agree on randomized encoding mappings. Surprisingly, in this setting, the adversarial sensors also need to coordinate, i.e., agree on an i.i.d. random sequence, denoted as $\{\theta(i)\}$, to generate the optimal jamming strategy. The saddle point solution of this problem is presented in the following theorem.

[1] An alternative practical method to coordinate is to generate the identical pseudo-random numbers at each sensor, based on pre-determined seed.

Theorem 1 ([2]). *The optimal encoding function for the transmitters is randomized uncoded transmission:*

$$X_m(i) = \gamma(i)\alpha_T U_m(i), \;\; M \geq m \geq 1 \tag{6}$$

where $\gamma(i)$ is i.i.d. Bernoulli ($\frac{1}{2}$) over the alphabet $\{-1, 1\}$

$$\gamma(i) \sim Bern(\frac{1}{2}). \tag{7}$$

The optimal jamming function (for adversarial sensors) is to generate i.i.d. Gaussian output

$$X_k(i) = \theta(i), \;\; M+K \geq k \geq M+1 \tag{8}$$

where

$$\theta(i) \sim \mathcal{N}(0, P_A), \tag{9}$$

and is independent of the adversarial sensor input $U_k(i)$. The optimal receiver is the Bayesian estimator of S given Y, i.e.,

$$h(Y(i)) = \frac{M\alpha_T\sigma_S^2}{M\alpha_T^2\sigma_S^2 + M^2\alpha_T^2\sigma_{W_T}^2 + K^2P_A + \sigma_Z^2}Y(i). \tag{10}$$

Cost at this saddle point as a function of the number of transmitter and adversarial sensors is:

$$J_C(M, K) = \sigma_S^2 \frac{M^2\alpha_T^2\sigma_{W_T}^2 + K^2P_A + \sigma_Z^2}{M\alpha_T^2\sigma_S^2 + M^2\alpha_T^2\sigma_{W_T}^2 + K^2P_A + \sigma_Z^2} \tag{11}$$

where $\alpha_T = \sqrt{\frac{P_T}{\sigma_S^2 + \sigma_{W_T}^2}}$.

The proof follows from verification of the fact that the mappings in this theorem satisfy the saddle point criteria given in (5).

Remark 1. Coordination is essential for adversarial sensors in the case of coordinating transmitters and receiver, in the sense that lack of adversarial coordination strictly decreases the overall cost.

3.2 No Coordination

In this section, we focus on the problem, where the transmitters do not have the ability to secretly agree on a random variable, i.e., "coordination" to generate their transmission function X_k. In this case, our analysis yields that the optimal transmitter strategy, which is almost surely unique, is uncoded transmission with linear mappings, while the adversarial optimal strategy for the (jamming) sensors is uncoded, linear mappings with the opposite sign of the transmitter functions. The following theorem presents our mail results associated with "no coordination" setting. A rather surprising observation is that the adversarial coordination is useless for this setting, i.e., even if the adversarial sensors can cooperate, the optimal mappings and hence the resulting cost at the saddle point does not change. Note however that, as we will show later, coordination capability of adversarial sensors is essential in the second extremal setting where transmitters are allowed to coordinate their choices.

Theorem 2 ([2]). *The optimal encoding function for the transmitters is uncoded transmission, i.e.,*

$$X_m(i) = \alpha_T U_m(i), \;\; M \geq m \geq 1 \tag{12}$$

The optimal jamming function (for adversarial sensors) is uncoded transmission with the opposite sign of the transmitters, i.e.,

$$X_k(i) = \alpha_A U_k(i), \;\; M+K \geq k \geq M+1 \tag{13}$$

The optimal decoding function is the Bayesian estimator of S given Y, i.e.,

$$h(Y(i)) = \frac{\left[(M\alpha_T + K\alpha_A)\sigma_S^2\right] Y(i)}{(M\alpha_T + K\alpha_A)\sigma_S^2 + M^2\alpha_T^2\sigma_{W_T}^2 + K^2\alpha_A^2\sigma_{W_A}^2 + \sigma_Z^2}. \tag{14}$$

Cost as a function of M and K is

$$J_{NC}(M,K) = \sigma_S^2 \frac{M^2\alpha_T^2\sigma_{W_T}^2 + K^2\alpha_A^2\sigma_{W_A}^2 + \sigma_Z^2}{(M\alpha_T + K\alpha_A)\sigma_S^2 + M^2\alpha_T^2\sigma_{W_T}^2 + K^2\alpha_A^2\sigma_{W_A}^2 + \sigma_Z^2} \tag{15}$$

where $\alpha_T = \sqrt{\frac{P_T}{\sigma_S^2 + \sigma_{W_T}^2}}$ and $\alpha_A = -\sqrt{\frac{P_A}{\sigma_S^2 + \sigma_{W_A}^2}}$.

The proof of theorem, can be found in [2], involves detailed information theoretic analysis and is omitted here for brevity. This problem setting implies a Stackelberg game where transmitters and the receiver play first as the Player 1, as they select their encoding functions. Then, Player 2 (the adversarial sensors), knowing the choice of Player 1, chooses its strategy.

Remark 2. Note that in this setting, the coordination capability for the adversaries do not help, in sharp contrast to the previous setting where, both transmitters and adversaries coordinate.

4 Main Result

The focus of this paper is the setting between the two extreme scenarios of coordination, namely full or no coordination. We assume that $M\epsilon$ transmitter sensors can coordinate with the receiver while $M(1-\epsilon)$ of them cannot coordinate. Similar to transmitters, only $K\eta$ of the adversarial sensors can coordinate while $K(1-\eta)$ adversarial sensors cannot coordinate. Let us assume, without loss of generality, that first $M\epsilon$ transmitters and $K\eta$ adversaries can coordinate. Let us also define the quantity ϵ_0 as the solution to:

$$J_C(M\epsilon_0, \sqrt{K^2\eta^2 + K(1-\eta)}) = J_{NC}(M,K) \tag{16}$$

The following theorem captures our main result.

Theorem 3. *If $\epsilon > \epsilon_0$, $M\epsilon$ capable transmitters use randomized linear encoding, while remaining $M(1-\epsilon)$ transmitters are not used.*

$$X_m(i) = \gamma(i)\alpha_T U_m(i), \quad M\epsilon \geq m \geq 1 \tag{17}$$

$$X_m(i) = 0 \quad M \geq m \geq M\epsilon \tag{18}$$

where $\gamma(i)$ is i.i.d. Bernoulli ($\frac{1}{2}$) over the alphabet $\{-1, 1\}$

$$\gamma(i) \sim Bern(\frac{1}{2}). \tag{19}$$

The optimal jamming policy (for the capable adversarial sensors) is to generate the identical Gaussian noise

$$X_k(i) = \theta(i), \quad M + K\eta \geq k \geq M + 1 \tag{20}$$

while remaining adversaries will generate independent Gaussian noise

$$X_k(i) = \theta_k(i), \quad M + K \geq k \geq M + k\eta \tag{21}$$

where

$$\theta_k(i) \sim \theta(i) \sim \mathcal{N}(0, P_A), \forall k \tag{22}$$

are independent of the adversarial sensor input $U_k(i)$.

If $\epsilon < \epsilon_0$, then the optimal encoding function for all transmitters is deterministic linear encoding, i.e.,

$$X_m(i) = \alpha_T U_m(i), \quad M \geq m \geq 1 \tag{23}$$

The optimal jamming function (for adversarial sensors) is uncoded transmission with the opposite sign of the transmitters, i.e.,

$$X_k(i) = \alpha_A U_k(i), \quad M + K \geq k \geq M + 1 \tag{24}$$

where $\alpha_T = \sqrt{\frac{P_T}{\sigma_S^2 + \sigma_{W_T}^2}}$ and $\alpha_A = -\sqrt{\frac{P_A}{\sigma_S^2 + \sigma_{W_A}^2}}$.

Proof. The transmitters have two choices: i) All transmitters will choose not to use randomization. Then, the adversarial sensors do not need to use randomization since the optimal strategy is deterministic, linear coding with the opposite sign, as illustrated in Theorem 2. Hence, cost associate with this option is $J_{NC}(M, K)$. ii) Capable transmitters will use randomized encoding. This choice implies that remaining transmitters do not send information as they do not have access to randomization sequence $\{\gamma\}$, hence they are not used. The adversarial sensors which can coordinate generate identical realization of the Gaussian noise while, remaining adversaries generate independent realizations. The total effective noise adversarial power will be $((K\eta)^2 + (1-\eta)K)P_A$, and the cost associated with this setting is $J_C(M\epsilon, \sqrt{K^2\eta^2 + K(1-\eta)})$. Hence, the transmitter will choose between two options depending on their costs,

$J_C(M\epsilon, \sqrt{K^2\eta^2 + K(1-\eta)})$ and $J_{NC}(M, K)$. Since, J_C is a decreasing function in M and hence in ϵ, whenever $\epsilon > \epsilon_0$, transmitters use randomization (and hence so do the adversaries), otherwise problem setting becomes identical to ”no coordination”. The rest of the proof simply follows from the proofs of Theorem 1 and 2 and is omitted here for brevity.

Remark 3. Note that in the first regime ($\epsilon > \epsilon_0$), we have a zero-sum game with saddle point. In the second regime ($\epsilon < \epsilon_0$), we have a Stackelberg game where all transmitters and receiver constitute the leader and adversaries constitute the follower.

5 Conclusion

In this paper, we presented new results on the game theoretical analysis of optimal communication strategies over a sensor network. Our recent prior [2] work had solved two extreme coordination cases where either all or none of the sensors coordinate. In this work, we focused on the setting where only a subset of the transmitter and/or jammer sensors can coordinate. We showed that the solution crucially depends on the number of transmitters and adversaries that can coordinate. In one regime, then the problem is a zero-sum game and admits a saddle point solution where transmitters with coordination capabilities use randomized linear encoding while the remaining the transmitter sensors are not used at all. Adversarial sensors that can coordinate generate identical Gaussian noise while other adversaries generate independent Gaussian noise. In the other regime, the problem becomes a Stackelberg game where the leader (all transmitter sensors) uses fixed (non-randomized) linear encoding while the follower (all adversarial sensors) uses fixed linear encoding with the opposite sign.

Our analysis has uncovered an interesting result regarding the mixed setting considered in this paper. The optimal strategy for transmitters sensors can be to discard the ones that cannot coordinate. Note that the coordination aspect of the problem is entirely due to game-theoretic considerations, which are also highlighted in this surprising result.

Several questions are currently under investigation, including extensions of the analysis to vector sources and channels, the asymptotic (in the number of sensors M and K) analysis of the results presented here; and extension of our analysis to asymmetric and/or non-Gaussian settings. An initial attempt to extend the results associated with the Gaussian test channel to non-Gaussian setting can be fond in [1].

Acknowledgments. This work was supported in part by the NSF under grants CCF-1016861, CCF-1118075 and CCF-1111342.

References

1. Akyol, E., Rose, K., Başar, T.: On optimal jamming over an additive noise channel. draft, `http://arxiv.org/abs/1303.3049`

2. Akyol, E., Rose, K., Başar, T.: Gaussian sensor networks with adversarial nodes. In: IEEE International Symposium on Information Theory. IEEE (2013)
3. Başar, T.: The Gaussian test channel with an intelligent jammer. IEEE Trans. on Inf. Th. 29(1), 152–157 (1983)
4. Başar, T., Wu, Y.: A complete characterization of minimax and maximin encoder-decoder policies for communication channels with incomplete statistical description. IEEE Trans. on Inf. Th. 31(4), 482–489 (1985)
5. Başar, T., Wu, Y.: Solutions to a class of minimax decision problems arising in communication systems. Journal of Optimization Theory and Applications 51(3), 375–404 (1986)
6. Bansal, R., Başar, T.: Communication games with partially soft power constraints. Journal of Optimization Theory and Applications 61(3), 329–346 (1989)
7. Gastpar, M.: Uncoded transmission is exactly optimal for a simple Gaussian sensor network. IEEE Trans. on Inf. Th. 54(11), 5247–5251 (2008)
8. Gastpar, M., Vetterli, M.: Power, spatio-temporal bandwidth, and distortion in large sensor networks. IEEE Journal on Selected Areas in Communications 23(4), 745–754 (2005)
9. Kashyap, A., Başar, T., Srikant, R.: Correlated jamming on MIMO Gaussian fading channels. IEEE Trans. on Inf. Th. 50(9), 2119–2123 (2004)
10. Shafiee, S., Ulukuş, S.: Mutual information games in multiuser channels with correlated jamming. IEEE Trans. on Inf. Th. 55(10), 4598–4607 (2009)