Distributed Detection with Censoring Sensors under Physical Layer Secrecy

Stefano Marano, Vincenzo Matta, Peter Willett, Fellow, IEEE

Abstract—We consider distributed binary detection problems in which the remote sensors of a network implement a censoring strategy to fulfill energy constraints, and the network works under the attack of an eavesdropper. The attacker wants to discover the state of the nature scrutinized by the system, but the network implements appropriate countermeasures to make this task hopeless. The goal is to achieve perfect secrecy at the physical layer, making the data available at the eavesdropper useless for its detection task. Adopting as performance metric certain Ali-Silvey distances, we characterize the detection performance of the system under physical layer secrecy.

Two communication scenarios are addressed: parallel access channels and a multiple access channel. In both cases the optimal operative points from the network perspective are found. The most economic operative solution is shown to lie in the asymptote of low energy regime. How the perfect secrecy requirement impacts on the achievable performances, with respect to the absence of countermeasures, is also investigated.

Keywords—Distributed detection, physical layer security, censoring nodes, attack countermeasure.

I. INTRODUCTION

DISTRIBUTED detection in Wireless Sensor Networks (WSNs) deals with the problem of efficient decision making based upon remotely collected observations, taking into account the communication constraints implied by data transmission [1]–[7]. As is well known, wireless networks are usually vulnerable to attacks by intruders of various nature, and there is no doubt that including security issues in the system design would be very desirable.

The emerging school of thought suggests that security in WSNs has to be addressed at the physical layer [8]. There exists a relevant bulk of works about physical layer security which is currently available, taking a genuine information theoretical perspective, and focusing on transmission-only problems, instead of detection ones. This problem can be traced back to the seminal ’75 work by Wyner [9] on the wiretap channel, where the tradeoff between the communication rate achievable by the legitimate user and the amount of information intercepted by the wiretapper is addressed. Obviously, Wyner’s viewpoint was certainly not focused on modern wireless networks, while, curiously, his models, formalization and results form the solid basis for the modern approach to physical layer security [10]–[13].

The reason for addressing the security issue at the physical layer is traditionally motivated by the fact that encryption and other higher-layer methods are typically unsuited to wireless networks, given the lack of infrastructure that characterizes them. However, we are interested in detection and, intriguingly, in this context the physical layer approach arises even from the opposite perspective. Indeed, suppose that the message content is either (i) perfectly secret thanks to message-encryption protocols, or (ii) inherently inaccessible due to structural limitations of the eavesdropper monitoring. Even in these cases, it is certainly very difficult for the system designer to avoid that an intruder may have access to some much coarser information, such as the channel accesses, and/or the transmission epochs of the messages in the network. In many scenarios of practical interest, as rough as they could be, such information is still relevant for detection purposes, especially when the number of sensors is large.

In this context, it is worth mentioning the emerging perspective, referred to as the detection of information flows, and the detection of encrypted stepping-stone connections, where, similarly to our setup, the only timing information is available, see the recent works by He and Tong [14]–[16]. They consider the problem of detecting a flow of information among the single units of a network, by simply having access to the time epochs of the packets at the different nodes. Also in that case, there is no possibility of having access to the message contents, but, nevertheless, non-trivial detection performances are shown to be achievable even with the rough information represented by the packet epochs.

In this work we address a detection problem in an energy-constrained wireless network, under physical layer secrecy constraints. We do not adhere to an information theoretical viewpoint, and instead elaborate on the commonly accepted paradigm of censoring sensors [17], [18] for energy-efficient distributed detection [19], [20] in sensor networks, by introducing the additional requirement for the system to be secure at the physical layer.

This is made in the following way. There is a communication channel connecting the sensors to a central unit (fusion center), and the aim of this latter is not to recover the remotely observed data, but to carry out a binary hypothesis test about the state of the nature that underlies the statistics of the observations. We shall consider both the cases of Parallel Access Channels (PAC) and of a Multiple Access Channel (MAC). In the former, each remote sensor is connected to the fusion center by a dedicated (and ideal) channel. In the latter, neighboring sensors are forced to share the same communication resource; we still assume that the common channel is ideal (in the sense of being noiseless), and focus on
the collision MAC with a simple slotted ALOHA protocol. The relevance of this model for detection in WSNs on a collision MAC is grounded in the recent cross-layer perspective adopted in [21].

As to the security aspects, we assume that an unauthorized intruder wants to make inference about the state of the nature exactly as the network does. Such an attacker senses the channel by monitoring the transmission activity of the sensors. It can perfectly discern between the ‘idle’ and the ‘busy’ state of the channel, and the collection of the transmission activities of the remote nodes constitutes the only set of data available to the eavesdropper to take its own decision. Therefore, the WSN adopts proper countermeasures to make the intruder data (idle/busy channel) useless for inference. This amounts to a perfectly secret system, which is the best operative modality for the network.

As said, the remote units of the system sense the environment and send messages to the fusion center. However, this data delivery is not for free. The nodes of WSNs are usually severely constrained in terms of their on-board power supplies, so that the energy spent for delivering data to the central unit is a serious constraint for the system designer [20]. According to the viewpoint pioneered by [17], we adopt as measure of the cost the transmission probability $\beta$, which is proportional to the per-sensor energy consumption, see also [18], [19], [22], [23]. This model is suitable for WSNs where the overhead usually associated to the communication task (channel access, connection setup, security/encryption, if any, etc.) is not negligible, and where each time a sensor wakes up attempting to transmit, a significant amount of energy is spent.

Note that, as standard in similar studies, our model obeys the perfect knowledge paradigm: the eavesdropper knows that the network is energy-constrained and implements the best censoring strategy and, on the other side, in adopting the proper countermeasures the network is aware of the operating modalities of the eavesdropper (i.e., its message-counting capability).

Figure 1 offers a conceptual scheme of the problem addressed, with reference to a single sensor of the network. The picture describes a single dedicated channel between the considered sensor and the fusion center, for the PAC architecture. On the other hand, it is also intended as representative of the MAC case, once the sensor’s transmission attempt has been successful. In the top panel, the general viewpoint of an intruder less powerful than the fusion center is emphasized by the presence of a degraded channel, while the energy constraints that each sensor must obey are embodied in the transmission policy block. In the bottom panel we expand the above general scheme: The binary output of the degraded channel models the idle/busy state; the sensor transmission policy amounts to sending the observed likelihood (outer linear region), or sending nothing (inner zero level).

We finally mention that, in the present paper, the detection performance metric is chosen within a sub-class of the Ali-Silvey distances, whose relevance for inference purposes is discussed in [24]. As a consequence, we shall see that a divergence-cost function naturally arises as one of our main analysis tool. Such a function, and the way we look at it, mirrors the well-known capacity-cost function that arises in the study of communication channels [25], [26]. Along the same line, the notion of divergence per unit cost, to be introduced shortly, is directly inspired to the concept of capacity per unit cost, introduced and popularized by [27].

Summarizing, the main actors on the scene are: (i) the performance metric, namely the divergence, say $D$; (ii) the energy consumption, quantified through the transmission probability $\beta$; (iii) the physical layer secrecy of the system with respect to unauthorized intruders having access to the network transmission activity. The goal of the designer is to maximize the overall divergence measured at the fusion center, with a constraint on the energy spent by the sensors, and with adequate protection against the intruder.

A. Main results

This paper formalizes the problem of an energy-constrained WSN engaged in a detection task, that we want to make perfectly secret against detection attempts made by an unauthorized eavesdropper.

For the PAC scenario, we introduce and characterize the divergence-cost function $D(\beta)$, that quantifies the system performance under perfect secrecy. It is proved that $D(\beta)$ is strictly increasing and strictly concave $\cap$ in the interior of $\beta \in (0,1)$. We also show that, for prescribed cost $\beta$, each sensor transmits only if its (local) likelihood ratio lies outside a no-send region in the form $(\tau_l(\beta), \tau_u(\beta))$, and there exists a unique pair of censoring thresholds $\tau_l(\beta), \tau_u(\beta)$, with $\tau_l(\beta) \leq 1$ and $\tau_u(\beta) \geq 1$. These functions are shown to be monotonic, and in the limit of vanishingly small $\beta$, the two thresholds converge to the extremes of the likelihood-pdf.
support. This corroborates and complements similar previous findings in the context of censoring, see e.g., [17].

Once the divergence-cost function has been characterized, we introduce the divergence per unit cost

$$D = \sup_{\beta} \frac{D(\beta)}{\beta},$$

whose operational meaning is that of characterizing the most economic way to convey information specifically suited for the detection task. It is shown that the divergence per unit cost is attained in the limit of vanishingly small per-sensor energy\(^1\): \(\beta \to 0\). This also reveals that the most economic way to deliver information for detection amounts using more and more sensors, with vanishing energy expense per each sensor.

For the MAC scenario, we specifically refer to a simple ALOHA collisions protocol in which \(m\) sensors share a common channel. For a fixed \(\beta\), larger values of \(m\) give a potential growth of information in the system, but, at the same time, increase the probability of collisions. We therefore take a cross-layer perspective in order to regulate the transmission activities. In the limit of \(m \to \infty\), we prove that the optimal operational point of the network is \(D/e\), thus providing further operational meaning to the divergence per unit cost.

The remainder of this paper is organized as follows. Section II, which addresses the PAC scenario, formalizes and solve the problem. In Sect. III the same tools are exploited for a multiple access environment. Section IV summarizes the main findings, while some mathematical derivations are postponed to the appendix.

II. Secure Detection over PAC

We consider a detection problem in which the remote units (nodes) of a WSN sense the surrounding environment and collect data to be delivered to a fusion center that must make the final decision about a binary hypothesis test of \(H_0\) against \(H_1\). The data collected at the remote nodes are assumed continuous random variables \(X_i\), \(i = 1, 2, \ldots, n\), where \(n\) is the number of sensors. These variables are independent and identically distributed (iid) under both the hypotheses, a simplifying assumption often adopted in similar studies, and generally accepted as a reasonable compromise between the accuracy of the mathematical model and its analytical tractability [1]. We denote by \(f_1(x)\) and \(f_0(x)\) the probability density functions corresponding to hypotheses \(H_1\) and \(H_0\), respectively. Further define the likelihood ratio \(Y_i = f_1(X_i)/f_0(X_i)\), whose pdfs under the hypotheses will be denoted by \(p_1(y)\) and \(p_0(y)\). It is immediate to recognize that \(Y_i\) are non-negative iid random variables. Whenever needed, we assume that \(p_1(y)\) and \(p_0(y)\) are sufficiently regular and smooth functions, in particular, they are continuous and well-behaved over the whole support, and there is no point-mass under either hypothesis. All the following analysis refers to the case that the common support of \(p_1(y)\) and \(p_0(y)\) is a connected set (line segment) defined as \((y_l, y_u)\), where clearly it is not excluded that \(y_l = 0\) and/or \(y_u = +\infty\).

As to the fusion center, it receives the vector of messages from the sensors and computes the global likelihood, say \(Y_{fc}\), which is used for a likelihood ratio test. This latter, as well-known, ensures the best performances according to many commonly adopted optimization criteria (e.g., Neyman-Pearson, Bayesian, minimax) [28]. As a proxy of the detection performances, we may refer to the the class of Csiszár \(f\)-divergences [24], [29], that is \(E_{H_0}(C(Y_{fc}))\), where \(C(y)\) is a continuous, convex \(\cup\), real-valued function defined for \(y > 0\), with \(C(1) = 0\). Throughout the paper, however, we restrict the analysis only to additive metrics with strictly convex \(C(y)\). This implies that the overall divergence perceived at the fusion center is simply the sum of the divergences measured at the remote nodes, and also that, thanks to Jensen’s inequality, the divergence is zero if and only if \(f_1(x) = f_0(x)\), but for zero-measure sets. The two Kullback-Leibler numbers \(D_{01}\) (set \(C(y) = y \log y\), logarithms are to base \(e\)) and \(D_{10}\) (set \(C(y) = - \log y\) and the \(J\)-divergence (the sum of the former two) fall in this class. The operative meaning of \(D_{01}\) and \(D_{10}\) is directly implied by Stein’s lemma [30], [31].

As to the remote nodes, we assume that each sensor has two possible alternatives: To transmit the observed likelihood \(y_i\) or to stay silent. The result is that it may be convenient for the sensors not to deliver those observations that appear less informative for discriminating between \(H_0\) and \(H_1\). This concept is quantified by the locally computed likelihood ratio \(y_i\): Sensors whose observations give very small or very large likelihoods send data (i.e., the likelihoods \(y_i\) themselves) to the fusion center, while the others stay silent, thus saving energy. Of course, this is the standard operative modality of WSNs with censoring nodes [17]–[19], [22]. The sending region of the \(i\)th sensor will be denoted by \(R_i\), and the corresponding transmission probabilities by \(\beta_i(i) = \Pr(y_i \in R_i)\), \(j = 0, 1\). We impose a balanced constraint such that both costs \(\beta_0(i)\) and \(\beta_1(i)\) at each sensor do not exceed a common value \(\beta\).

The local divergence perceived at each sensor is

$$D_i = \int_{R_i} p_0(y)C(y)dy + (1 - \beta_0(i))C \left(\frac{1 - \beta_1(i)}{1 - \beta_0(i)}\right), \quad (1)$$

and, according to the above discussion, the goal of the designer is that of maximizing the global divergence \(\sum_{i=1}^{n} D_i\) with the per-sensor constraint \(\max\{\beta_0(i), \beta_1(i)\} \leq \beta, \forall i\).

The eavesdropper has no access to the data received from the fusion center, but it can monitor the transmission activity of the sensors. In this respect, its detection capabilities are those of testing the binary pmfs corresponding to the idle/busy channel information. The divergence achieved by the eavesdropper is accordingly

$$D_{eav} = \sum_{i=1}^{n} \beta_0(i)C \left(\frac{\beta_1(i)}{\beta_0(i)}\right) + (1 - \beta_0(i))C \left(\frac{1 - \beta_1(i)}{1 - \beta_0(i)}\right).$$

To take into account the different constraints imposed to our

\(^1\)The capacity per unit cost studied by Verdú [27] shares the same property, when the channel has a free input symbol.
system, let us consider the following optimization problem:

$$\begin{align*}
\text{maximize} & \quad \sum_{i=1}^{n} D_i \\
\text{subject to} & \quad \max\{\beta_1(i), \beta_0(i)\} \leq \beta \quad \forall i \\
& \quad D_{\text{avail}} \leq \Delta.
\end{align*}$$

We note explicitly that, as to the energy constraint $\beta$, different choices deserved attention in the topical literature. For instance, one could impose the constraint only under $\mathcal{H}_0$, that is, $\beta_0 \leq \beta$, motivated by physical considerations, as reported in [17].

With respect to (2), it is understood that the specific case that the intruder is completely blind deserves particular attention. As a matter of fact, in the wiretap channel literature it is typical to consider the maximum degree of information achieved by the main user (fusion center, in our terminology), while the information of the eavesdropper is exactly zero. This is commonly referred to as a regime of perfect secrecy [9]: We want to maximize the divergence seen at the fusion center subject to $\max\{\beta_1(i), \beta_0(i)\} \leq \beta$, $\forall i$, and $\Delta = 0$. Addressing this issue is the main theme of this work.

It is worth noting that designing the system to get the maximum divergence compatible with only an energy limitation, would in general give to the intruder some detection capability. To avoid this, we are here faced with a maximization on the subspace allowing perfect secrecy. This reduction of the search space, which arises as a natural consequence of the physical layer security issue, has the additional benefit of simplifying the mathematical analysis, providing clean analytical results, as detailed in the forthcoming sections.

### A. Divergence-cost function

In order to ensure perfect secrecy, $\Delta = 0$, we must impose $\beta_0(i) = \beta_1(i)$, $\forall i$. The optimization of the global divergence in eq. (2) can be accordingly recast as

$$\begin{align*}
\text{maximize} & \quad \sum_{i=1}^{n} D_i \\
\text{subject to} & \quad \beta_1(i) = \beta_0(i) \leq \beta \quad \forall i.
\end{align*}$$

Due to the additive structure of the objective function, and the balanced per-sensor cost used here, the problem decouples such that it suffices to maximize the local divergence $D_i$, yielding:

$$D(\beta) \overset{\text{def}}{=} \max_{\beta_1 = \beta_0 \leq \beta} \int_{\mathbb{R}} p_0(y)C(y)dy,$$

where index $i$ is omitted, and the dependence of the maximum available divergence on the maximum available cost $\beta$ has been made explicit. Note that the second term in eq. (1) disappears due to the condition $\beta_0(i) = \beta_1(i)$.

The function defined in (3) will be referred to as divergence-cost function and plays a major role in our analysis: under perfect secrecy each sensor contributes by an amount of $D(\beta)$ to the overall detection performance, which therefore amounts to $nD(\beta)$.

Before stating the main theorem pertaining to the PAC case, we need to characterize the censoring regions. Recall that we want to maximize the detection performance of the WSN, with a prescribed constraint on the energy spent by the sensors (transmission probability $\beta$), and also ensuring that the intruder is given no chance to infer the state of the nature ($\mathcal{H}_0$ or $\mathcal{H}_1$). This setting is formalized by the optimization problem (3), where the search is carried out over all possible sending regions $\mathcal{R}$. However, in the standard censoring literature it is shown that the optimal censoring strategy amounts activating the transmission of the local likelihoods $y_i$, falling outside a certain singly-connected region. This property holds for a large class of performance figures, including those here considered, and is a consequence of the convexity of the function $C(y)$, see [17, Th. 3]. For all $\beta$, the maximum divergence is thus always obtained with a no-send region which is a single interval, say $y \in [\tau_l, \tau_u]$. Accounting for the above property, the costs become

$$\beta_j = \int_{y_l}^{\tau_l} p_j(y)dy + \int_{\tau_u}^{y_u} p_j(y)dy, \quad j = 0, 1,$$

and the objective function to be maximized is

$$\int_{y_l}^{\tau_l} p_0(y)C(y)dy + \int_{\tau_u}^{y_u} p_0(y)C(y)dy.$$

The following lemma characterizes the censoring regions.

**LEMMA.** Let $\beta \in (0, 1)$ be the energy constraint. The unique pair of censoring thresholds $[\tau_l(\beta), \tau_u(\beta)]$ is such that $\tau_u(\beta)$ is a strictly decreasing function ranging from $y_u$ to 1, while $\tau_l(\beta)$ is a strictly increasing function ranging from $y_l$ to 1.

The proof is given in the appendix.

We are now ready for stating the main result of this section.

**THEOREM 1.** The divergence-cost function $D(\beta)$ is strictly increasing and strictly concave $\forall \beta \in (0, 1).

The proof is given in the appendix. The typical shape of $D(\beta)$ is shown in Fig.2.

**Remark.** The concavity of $D(\beta)$ has important implications. For example, let us suppose that a fraction $\alpha'$ of the sensors works with a cost constraint $\beta'$, and the remaining fraction $\alpha'' = 1 - \alpha'$ works with constraint $\beta''$. With $\alpha'\beta' + \alpha''\beta'' = \beta$ an overall cost of $\beta$ is achieved, and the total divergence result in $\alpha'D(\beta') + \alpha''D(\beta'')$. The strict concavity of the divergence-cost implies that this latter quantity is less than $D(\beta)$, which
can be attained by imposing one and the same constraint \( \beta \) to all the sensors. More generally, there is no advantage in working with heterogeneous cost constraints.

**Remark 2.** An immediate way to obtain a perfect secret system would be to make the sensors’ transmission probability independent of the measured data. Suppose for instance that no censoring is imposed and that each node simply delivers its local likelihood with an a-priori fixed probability \( \beta \). The average performance of the system is \( \beta D(1) \), because the sensors are active (on the average) and the contribution of uncensored delivering amounts to the divergence-cost function, when the cost is set to its upper limit 1. Clearly, such a dumb scheme obeys a cost constraint \( \beta \). Exactly the same constraint, however, is attained by using the censored strategy with results, as we have seen, in a detection performance of \( D(\beta) \). Now, a simple consequence of Theorem 1 is that \( D(\beta)/\beta \) decreases with \( \beta \), which implies \( D(\beta) > \beta D(1) \), meaning that the less clever approach of a blind limitation of the sensors’ transmissions is by a large margin sub-optimal.

It is easily seen that the same remains true also if one obtains the desired cost \( \beta \) by transmitting with probability \( \alpha \) the likelihoods censored at level \( \gamma \). More explicitly, suppose that we design the censoring strategy in order to obtain a per-sensor performance of \( D(\gamma) \), which correspond to a cost \( \gamma > \beta \). Then to fit the cost constraint, the transmission is actually enabled (irrespective of the data) with a probability \( \alpha \) such that \( \beta = \alpha \gamma \). The performance of such scheme is \( \alpha D(\gamma) \), which is less than \( D(\beta) \), since \( \alpha D(\gamma) = \alpha \gamma D(\alpha \gamma)/\gamma < D(\alpha \gamma) \). Therefore, Theorem 1 ensures that no advantage can be obtained.

**Remark 3.** We explicitly note that the proved properties of the divergence-cost \( D(\beta) \) rely essentially on the convexity of \( C(y) \), that is, they hold true for the whole class of Csiszár f-divergences [29]. What, instead, fails to be true in general, is that the maximization of the overall divergence available at the fusion center, is achieved by maximizing the local divergence as in eq. (3).

Two points should be emphasized. On one hand, focusing on \( D(\beta) \) as a global performance metric certainly makes sense for all the separable \( f \)-divergences [32], not necessarily only the additive ones. On the other hand, even when the global optimization does not decouple, maximizing, e.g., the sum of the local divergences may be appealing for practical reasons, especially when the number of sensors is large, see [19].

### B. Divergence per unit cost

We define the **divergence per unit cost** as the best value of the ratio \( D(\beta)/\beta \):

\[
D \overset{def}{=} \sup_{\beta} \frac{D(\beta)}{\beta}. \tag{4}
\]

This quantity mirrors the capacity per unit cost popularized by Verdú in his seminal work [27], whose definition relies upon the well-known capacity-cost function (see [26]), exactly as we define \( D \) through \( D(\beta) \).

The characterization of the divergence per unit cost \( D \) is now in order. Recalling definition (4), since \( D(\beta) \) is non-negative, strictly concave \( \gamma \), and \( D(0) = 0 \), we get

\[
D = \lim_{\beta \to 0} \frac{D(\beta)}{\beta}, \tag{5}
\]

provided that this latter limit exists (finite or infinite). Now, while \( D \) is a measure of the detection performance of the WSN per single sensor, \( D \) characterizes the performance per unit cost, and from eq. (5) we see that the most **economic** way to deliver information for discriminating between the two hypotheses, is that of working in the limit of vanishing \( \beta \). As \( \beta \) goes to zero, the no-send region coincides with the support of the likelihoods’ pdf, implying that, for any fixed \( n \), the overall divergence goes to zero: Delivering zero-energy cannot provide any successful transfer of information, as we expect. More interesting is the case that \( \beta \to 0 \) and \( n \to \infty \), in such a way that the product \( n \beta \) stays constant. Assuming for simplicity that \( \beta = 1/n \), the overall system performance is

\[
\lim_{\beta \to 0} nD(\beta) = \lim_{\beta \to 0} \frac{D(\beta)}{\beta} \tag{6}
\]

so that \( D \) rules the asymptotic detection capabilities of the WSN.

The divergence per unit cost \( D \) can be evaluated by using the first derivative

\[
\delta(\beta) \overset{def}{=} \frac{dD(\beta)}{d\beta}, \]

since \( \lim_{\beta \to 0} D(\beta)/\beta = \lim_{\beta \to 0} \delta(\beta) \). From the explicit expression of \( \delta(\beta) \) in eq. (16) of the appendix, by recalling that, as \( \beta \) vanishes, the two censoring thresholds tend to the extremes of the pdf’s support, we can work out the required limit. First, assuming that \( \lim_{\beta \to 0} \delta(\beta) \) is finite, we get

\[
D = \frac{1 - y_1}{y_u - y_1} C(y_u) + \frac{y_u - 1}{y_u - y_1} C(y_l). \tag{7}
\]

On the other hand, it may also happen that the above limit is infinite when, e.g., \( y_u = \infty \) and/or \( y_l = 0 \). For instance, let \( y_l = 0 \) and \( y_u = \infty \) and consider

\[
C_{10}(y) = y \log y, \quad C_{01}(y) = \log \frac{1}{y},
\]

namely, the two Kullback-Leibler distances \( D(\mathcal{H}_1||\mathcal{H}_0) \) and \( D(\mathcal{H}_0||\mathcal{H}_1) \), respectively [31]. For vanishingly small \( \beta \), we get

\[
\delta_{10}(\beta) \sim \log \tau_u(\beta) \quad \text{and} \quad \delta_{01}(\beta) \sim \log \frac{1}{\tau_l(\beta)},
\]

which both diverge for \( \beta \to 0 \).

### C. Examples

The characterization provided in the previous sections is now exploited to address study cases of relevance for practical applications. On one hand, (i) this allows checking the predicted behavior of the divergence function \( D(\beta) \) and the relevant properties of the divergence per unit cost; on the other hand, (ii) inspection of particular examples will help
in understanding how much is lost by imposing the secrecy requirement.

It seems quite natural to address the classical Gaussian shift-in-mean problem, and we made this for different problem parameters (e.g., different signal-to-noise ratios). However, as far as we can tell, the evaluation of the censoring thresholds needed to work out the divergence-cost function requires numerical computations. It turns out that little physical/general insights are obtained, and we accordingly choose not to detail the numerical evidences, limiting ourselves to summarize the main findings.

As to point (i), the expected properties of \( D(\beta) \) have been of course verified. More importantly, as to issue (ii), we made the comparison of \( D(\beta) \) with the divergence corresponding to the case that the perfect secrecy constraint is relaxed, say \( \Delta(\beta) \). For the Gaussian case with the elected symmetric cost constraint \( \max\{\beta_0, \beta_1\} \leq \beta \), we found, for different signal-to-noise-ratios, that the maximum divergence is always obtained for equal costs \( \beta_0 = \beta_1 \); this implies that nothing is lost by imposing the secrecy constraint. As a further check, we also considered the asymmetric cost constraint imposed only under the null hypothesis, that is \( \beta_0 \leq \beta \), and, as expected, for this case \( \Delta(\beta) > D(\beta) \), and the equality is lost.

From the previous numerical evidences, it seems that the absence of loss in working with \( D_{\text{av}} \) is related to the symmetries of both the Gaussian shift-in-mean detection problem, and the imposed cost constraint, while, in general, we expect that such something should be paid by requiring perfect secrecy. This pushes us to investigate a different case of practical interest, that is, the well-known exponential shift-in-scale problem. We assume

\[
f_0(x) = e^{-x} u(x), \quad f_1(x) = \frac{1}{1 + \theta} e^{-\frac{x}{1+\theta}} u(x),
\]

where \( u(x) \) is the unit-step function. The corresponding likelihood ratio is thus computed as

\[
y = \frac{f_1(x)}{f_0(x)} = \frac{1}{1 + \theta} e^{\frac{x}{1+\theta}} u(x),
\]

such that the extremal points are \( y_l = (1 + \theta)^{-1} \) and \( y_u = \infty \). Referring for simplicity to \( z = \log y \), it is easily recognized that the log-likelihood \( z \) is a shifted exponential random variable, that is

\[
q_0(z) = \frac{1}{a_0} e^{-\frac{z - \log y_l}{a_0}} u(z - \log y_l),
\]

\[
q_1(z) = \frac{1}{a_1} e^{-\frac{z - \log y_u}{a_1}} u(z - \log y_u),
\]

with \( a_0 = \theta/(1 + \theta) \), and \( a_1 = \theta \). The costs \( \beta_0 \) and \( \beta_1 \) become

\[
\beta_0 = 1 - \left( \frac{y_l}{\tau_l} \right)^{1+1/\theta} + \left( \frac{y_l}{\tau_u} \right)^{1+1/\theta}, \quad (8)
\]

and

\[
\beta_1 = 1 - \left( \frac{y_l}{\tau_l} \right)^{1/\theta} + \left( \frac{y_l}{\tau_u} \right)^{1/\theta}. \quad (9)
\]

We solve numerically the equations \( \beta_1 = \beta_0 = \beta \), getting the values of the thresholds \( \tau_l(\beta) \) and \( \tau_u(\beta) \).

![Fig. 3. The divergence-cost function \( D(\beta) \) (curve in bold), versus the cost \( \beta \), for the exponential example with \( \theta = 1 \). Also shown are the curves pertaining to a system without security countermeasure: \( D_{\text{unc}}(\beta) \) is the divergence experienced by the network (dashed curve), while \( \Delta(\beta) \) is the correspondent (nonzero) divergence attainable by the eavesdropper (shown by the tiny solid curve). Panel (a) refers to the Kullback-Leibler distance between \( \mathcal{H}_0 \) and \( \mathcal{H}_1 \), while panel (b) shows the case of the Kullback-Leibler distance between \( \mathcal{H}_1 \) and \( \mathcal{H}_0 \).](image:Fig. 3. The divergence-cost function \( D(\beta) \) (curve in bold), versus the cost \( \beta \), for the exponential example with \( \theta = 1 \). Also shown are the curves pertaining to a system without security countermeasure: \( D_{\text{unc}}(\beta) \) is the divergence experienced by the network (dashed curve), while \( \Delta(\beta) \) is the correspondent (nonzero) divergence attainable by the eavesdropper (shown by the tiny solid curve). Panel (a) refers to the Kullback-Leibler distance between \( \mathcal{H}_0 \) and \( \mathcal{H}_1 \), while panel (b) shows the case of the Kullback-Leibler distance between \( \mathcal{H}_1 \) and \( \mathcal{H}_0 \).)

Let us now consider the case of a Kullback-Leibler distance between \( \mathcal{H}_1 \) and \( \mathcal{H}_0 \), i.e., \( C(y) = y \log y \). Substituting into the divergence, we have:

\[
D(\beta) = \int_{\log y_l}^{\log y_u} q_1(z) z e^z dz + \int_{\log \tau_u(\beta)}^{\infty} q_1(z) z e^z dz.
\]

Taking the limit \( y_u \to \infty \) in eq. (7) tells that \( D_{10} = \infty \).

The above analysis is repeated for the case of the other Kullback-Leibler distance, namely assuming \( C(y) = -y \log y \). A basic difference here is that the divergence per unit cost is finite. Indeed, again evaluating eq. (7) in the limit of large \( y_l \) gives, for the considered example of \( \theta = 1 \), \( D_{01} = \log 2 \).

A natural question at this point is about how much is lost by imposing the perfect secrecy constraint. Otherwise stated, what would be the gap between our \( D(\beta) \) and the divergence obtained by optimizing the censoring thresholds without care about the eavesdropper, as done, e.g., in [17]? As already discussed, the additive nature of the divergence, along with the per-sensor cost, allows working in terms of the per-sensor divergence \( D_s \), and we do this. Specifically, we maximize the per-sensor divergence for a prescribed cost limitation \( \max\{\beta_0, \beta_1\} \leq \beta \), without any constraint imposed on the divergence perceived by the eavesdropper side. As done before, we accordingly denote the optimized quantity by the symbol \( D_{\text{unc}}(\beta) \). As to the intruder, different from the previous analysis, in this setup it will exhibit in general non-zero detection capabilities. We shall denote the per-sensor divergence seen by the eavesdropper with \( \Delta(\beta) \).

In Fig. 3 we display the three relevant quantities \( D(\beta) \), \( D_{\text{unc}}(\beta) \) and \( \Delta(\beta) \), for the case of the two Kullback-Leibler numbers. Note that, at the extreme points \( \beta = 0, 1 \), the costs under different hypotheses must obviously coincide. This implies that \( D(0) = D_{\text{unc}}(0) \), \( D(1) = D_{\text{unc}}(1) \) and \( \Delta(0) = \Delta(1) = 0 \).

Let us first compare the two curves \( D(\beta) \) and \( D_{\text{unc}}(\beta) \). We see that \( D_{\text{unc}}(\beta) \geq D(\beta) \), and this is obvious. What is
behaviorally. This seems to suggest that, when resources to be exactly quadratic (Fig. 4D), the behavior of particular values of the parameters considered in the example, two curves: it is remarkable that the loss due to the secrecy not so obvious is the relatively small distance between the In the low-cost regime, $\beta$ about both the transmission activities and the message content. Hii case of the Kullback-Leibler distance between $D$ yielding the difference between the performance of the network and the performance of the eavesdropper in presence (solid curve) and in absence (dashed) of the perfect secrecy countermeasure. Therefore, the solid curve represents $\Delta(\beta)$, and the dashed is $D_{\text{unc}}(\beta) - \Delta(\beta)$. As for Fig. 3, panel (a) refers to the Kullback-Leibler distance between $H_0$ and $H_1$, while panel (b) shows the case of the Kullback-Leibler distance between $H_1$ and $H_0$.

not so obvious is the relatively small distance between the two curves: it is remarkable that the loss due to the secrecy requirement, in terms of detection performance, is modest.

Switching to the analysis of $\Delta(\beta)$, we observe that $\Delta(\beta) \leq D_{\text{unc}}(\beta)$, as we expect since the network has information about both the transmission activities and the message content. In the low-cost regime, $\beta \to 0$, the curves $D_{\text{unc}}(\beta)$ and $\Delta(\beta)$ behave similarly. This seems to suggest that, when resources are scarce, the best detection is achieved by looking at the transmission activities, rather than the message content.

A different behavior seems to arise for large costs. In this regime the details available about the message information give a substantial improvement with respect to the simple message-counting available at the eavesdropping side.

Summarizing, the above analysis emphasizes that, for the considered case study, i) the loss in terms of detection exponent is modest and ii) the lack of countermeasures may be dangerous, especially in the low-cost regime.

It is also of interest to compare the difference between the (per-sensor) divergence of the network and the (per-sensor) divergence of the eavesdropper, for the two distinct schemes under consideration: presence and absence of security constraints. This is explicitly done in Fig. 4. We stress that, for the considered scenario, the curve $D(\beta)$ (recall that the eavesdropper has zero divergence in this case) stays always above the difference $D_{\text{unc}}(\beta) - \Delta(\beta)$. Interestingly, for the particular values of the parameters considered in the example, the behavior of $D_{\text{unc}}(\beta) - \Delta(\beta)$ can be analytically verified to be exactly quadratic (Fig. 4(a)) and linear (Fig. 4(b)), but this cannot be taken as the general rule.

III. DETECTION-SECURE ACCESS OVER COLLISION CHANNELS

In this section we look at the problem of distributed detection with physical layer secrecy, in the context of WSNs where the communication between sensors and a central unit involves a MAC. We borrow the cross-layer viewpoint and the physical model from [21], which is well-suited to a detection-centric perspective of the multiple access and, as done for the case of parallel channels, the further requirement of secrecy is accounted for.

Let us specify the model, first. Suppose that a field of tiny, cheap, possibly unreliable and battery-limited sensors is monitoring a feature, and is eager to deliver its observations to the fusion center according to the SENMA (Sensor Networks with Mobile Agents) concept [33]. The latter architecture, which we are going to briefly describe, is chosen due to its potential efficiency in terms of energy spent for communication, with respect to other protocols (e.g., multiphase in flat ad-hoc networks), other than for its properties of versatility, scalability, robustness, etc. Specifically, a roving base-station queries the sensors in a certain footprint area by emitting a polling signal. The medium connecting the sensors to the mobile FC is modelled as a multiple access collision channel, and all sensors within the rover’s field of view, when queried, respond according to the (simplest version of) the slotted ALOHA policy [34]: if more than one message attempts to transmit, then the message is lost; otherwise the message is assumed to be received correctly. To simplify the analysis it is assumed, as suggested in [21], that different snapshots involve different sensors. This working hypothesis gives insights on the system performance and optimization, and it is also expected to provide accurate results for relatively large number of sensors.

Complying with the same cross-layer philosophy exploited in [21], here we choose to tune the ALOHA transmission probability of each sensor on a detection-centric basis. Specifically, a network node self-regulates its own accesses by censoring the less-informative likelihoods, i.e., the channel access is attempted only if the likelihood lies inside the send-region $R_i$. A general analysis allowing each sensor in the field of view to use different regions is rather involved. For this reason, and without claiming a full generality, in the following we assume that the transmission policy is one and the same for all sensors in the single rover’s snapshot, $R_i = R, \forall i$. Furthermore, due to the symmetry of the constraints imposed to all sensors in the network, the policy does not change over different snapshots, and the problem reduces to the maximization of the per-snapshot divergence, say $D_{\text{h}}(m)$, for a given number of per-snapshot sensors $m$. As before, an eavesdropper is assumed to overhear the system by monitoring the transmission attempts.

The goal of the designer is to maximize the detection performance $D_{\text{h}}(m)$, while ensuring perfect secrecy. It would clearly be desirable to fully exploit the available $m$ sensors by letting the detection performances to grow with $m$. To get this, we must take into account the presence of collisions over the channel in such a way that each sensor self-regulates its own transmission probability (i.e., the censoring thresholds) as a function of $m$. A tradeoff clearly arises in that the detection performances would benefit from receiving as much data as possible, but, if the transmission activity is too high, it is

The assumption of working with the SENMA architecture is not restrictive: the actions taken by the mobile fusion center can be as well implemented by a fixed fusion center, in some equivalent fashion. We refer to the SENMA mainly for concreteness.
unlikely that one sensor could successfully communicate with the mobile agent.

At first glance it may appear that we are disregarding the energy constraint, while focusing only on the number of sensors per snapshot. However, this choice is motivated by the fact that, as just observed, the per-sensor cost will be automatically limited by the collisions, and, as we shall prove, it will be approximately in the order of \(1/m\).

Let us now state the main result on the collision MAC with distributed secure detection.

**Theorem 2.** The per-snapshot divergence \(D_a(m)\) verifies
\[
\lim_{m \to \infty} D_a(m) = \frac{D}{e},
\]
where \(D\) is the divergence per unit cost, \(1/e\) is the throughput of the considered slotted ALOHA access protocol, and \(m\) is the number of sensors in a single query. The case that \(D\) is infinite is contemplated.

The proof is given in the appendix.

Assume that each sensor in a single snapshot uses a transmission probability \(\beta_{0,1}\), which in general depends upon the hypothesis. Accounting for the collision model, the probability density of the likelihood received at the fusion center, evaluated in a point belonging to the send-region, is simply
\[
m(1 - \beta_{0,1})^{m-1} p_j(y), \quad j = 0, 1.
\]
By integrating the above over the send-region \(R\), we get the overall probability of getting data at the fusion center in a single query: \(m(1 - \beta_{0,1})^{m-1} \beta_{0,1}\), which must be enforced to be the same under the two hypotheses in order to fulfill the perfect secrecy requirement. This imposes, as expected, \(\beta_{0} = \beta_{1} = \beta\). Moreover, the divergence per single snapshot only contains the term related to eq. (10), and amounts to
\[
m(1 - \beta)^{m-1} \int_{R} p_0(y) C(y) dy.
\]
Now, from the results in the previous sections, we know that, for each \(\beta \in (0, 1)\), the send-region \(R\) should be selected as a connected region in order to maximize the divergence, and that a unique pair of thresholds exists yielding
\[
D_a(\beta, m) \overset{\text{def}}{=} m(1 - \beta)^{m-1} D(\beta).
\]
The above expression shows that it is no longer true that each sensor should use the maximum available transmission probability, as happens in the presence of collisions. Indeed, consider the limiting case of \(\beta = 1\), due to the presence of collisions on the channel, \(D_a(1, m) = 0, \forall m > 1\).

It turns out, instead, that each sensor should select the most convenient \(\beta\). Clearly, the solution is one and the same for all sensors, and corresponds to maximize the above \(D_a(\beta, m)\) with respect to \(\beta\), and the maximum divergence per single snapshot can be defined as
\[
D_a(m) \overset{\text{def}}{=} \max_{\beta} D_a(\beta, m) = m[1 - \beta_m^*]^{m-1} D(\beta^*_m),
\]
where \(\beta_m^*\) is just the maximizer. In general, this problem will not admit a simple closed-form solution. We shall thus focus on the case that the number of sensors per rover’s query \(m\) is large enough.

First, let us investigate the behavior of \(\beta_m^*\). From eq. (11) we can write
\[
D_a(m) \leq m[1 - \beta_m^*]^{m-1} D(1),
\]
the upper bound following from having substituted the divergence-cost with its maximum attained when the argument is unitary. This reveals that \(\beta_m^*\) must vanish as \(m \to \infty\), as otherwise the available divergence would go to zero, that is, for large \(m\), the system is forced to work in the low-cost regime.

We can summarize the above analysis by saying that in the case of accesses by the ALOHA protocol, the sensors’ energy constraint are somehow replaced (or self-regulated) by the physical limitations imposed by the collisions occurring over the channel. The optimal operative point, in the limit of large \(m\), is the low-cost regime of \(\beta \to 0\). Theorem 2 proves that the divergence per unit cost \(D\) arises as natural performance proxy; in particular the divergence attained at the mobile agent per single snapshot is asymptotically \(D/e\).

The same exponential example addressed in the previous section with reference to the parallel architecture, is now considered for the MAC scenario. The maximum per-snapshot divergence \(D_a(m)\) achievable with \(m\) candidate per-snapshot sensors is shown in Fig. 5. Comfortably, the optimal transmission probability \(\beta_m^*\) guarantees a monotonic growth of the detection performance with the available sensor density. Such a desired behavior comes from a careful detection-centric managing of the MAC collisions, provided by our cross-layer design.

We know that \(D_a(m)\) must converge to \(D/e\), and we get this. Indeed, in the left panel of Fig. 5, where the Kullback-Leibler distance between \(\mathcal{H}_0\) and \(\mathcal{H}_1\) is considered, \(D_{01} = \log 2\) and accordingly \(D_a(m)\) approaches \(\log 2/e \approx 0.255\). The right panel refers to the Kullback-Leibler distance between \(\mathcal{H}_1\) and \(\mathcal{H}_0\), and, as already noticed, \(D_{10}\) is infinite, and, accordingly, \(D_a(m)\) grows indefinitely.
IV. SUMMARY

In a WSN engaged in a binary detection task, the remote nodes sense the environment and deliver messages to the fusion center for the decision. The main system constraint is the energy $\beta$ spent for the communication task from the sensors, and a censoring protocol is thus imposed to mitigate that burden. We address two different scenarios for the communication between sensors and fusion center, namely, the case of parallel access channels (PAC) and that of a single multiple access channel (MAC) with a slotted ALOHA protocol.

The wireless nature of the system makes it very vulnerable to intrusion attacks: An unauthorized entity senses the wireless channel and monitors the transmission activity of the sensors with the aim of making the same binary inference of the WSN. The system adopts a drastic attack countermeasure: It is designed in such a way that the intruder is made completely “blind”. We give no chance of inference to the attacker by making its data useless for guessing the state of the nature, by enforcing a perfect secrecy requirement at the physical layer.

For the PAC model, we characterize the information sources (sensors) in terms of a certain divergence function $D(\beta)$, e.g., the well-known Kullback-Leibler distance. Its monotonicity and concavity properties as function of $\beta$ are studied in due depth and the related physical implications are emphasized. The concept of divergence per unit cost is introduced, and the relevant properties and operative meaning are discussed.

For the MAC case, we propose a cross-layer approach which focuses on a detection-centric perspective, in order to obtain an efficient management of the channel collisions that maximizes the network detection performance. We prove that the maximum divergence compatible with a given sensor density is ruled by the previously introduced divergence per unit cost, scaled by the classical ALOHA throughput $1/e$.

APPENDIX

A. Results for the PAC case

The optimization problem is that of determining the censoring thresholds $\tau_l$ and $\tau_u$ which solve

\[
D(\beta) = \max \left\{ \int_{y_l}^{\tau_l} p_0(y)C(y)dy + \int_{\tau_u}^{y_u} p_0(y)C(y)dy \right\},
\]

\[
\int_{y_l}^{\tau_l} [p_0(y) - p_1(y)]dy = -\int_{\tau_u}^{y_u} [p_0(y) - p_1(y)]dy,
\]

\[
\int_{y_l}^{\tau_l} p_0(y)dy + \int_{\tau_u}^{y_u} p_0(y)dy = \beta,
\]

where the second equation serves to fulfill the perfect secrecy requirement. As it can be seen from the third equation, we study the problem with an equality constraint, and then verify that $D(\beta)$ is strictly increasing for $\beta \in (0, 1)$. This ensures that $D(\beta)$ so computed is in fact the true maximum. Since

\[
\int_{y_l}^{y_u} [p_0(y) - p_1(y)]dy = 0,
\]

the above can be recast as

\[
D(\beta) = \max \left\{ \int_{y_l}^{\tau_l} p_0(y)C(y)dy + \int_{\tau_u}^{y_u} p_0(y)C(y)dy \right\},
\]

\[
\int_{y_l}^{\tau_l} [p_0(y) - p_1(y)]dy = \int_{\tau_u}^{y_u} [p_0(y) - p_1(y)]dy,
\]

\[
\int_{y_l}^{\tau_l} p_0(y)dy + \int_{\tau_u}^{y_u} p_0(y)dy = \beta.
\]

Proof of the Lemma. By defining $g(y) = p_0(y) - p_1(y)$, the second equation in (12) can be written

\[
\int_{y_l}^{\tau_l} g(y)dy = \int_{\tau_u}^{y_u} g(y)dy.
\]

By introducing the function $h(\tau) = \int_{y_l}^{\tau} g(y)dy$, the relationship between $\tau_l$ and $\tau_u$ amounts to impose $h(\tau_l) = h(\tau_u)$. Now, $h(\tau)$ has the following (immediate) properties: $h(y_l) = h(y_u) = 0$, and $dh(\tau)/d\tau = g(\tau)$. From the nesting property of the likelihood ratio [35, p. 44], we further know that $p_1(y)/p_0(y) = y$, yielding

\[
g(y) = p_0(y)(1 - y)
\]

that is, $h(\tau)$ is strictly increasing for $\tau < 1$, and strictly decreasing for $\tau > 1$, with a maximum $h(1) = \int_{y_l}^{y_u} g(y)dy > 0$.

In view of the above properties, the condition $h(\tau_l) = h(\tau_u)$ can be pictorially illustrated as in Fig. 6. For $\beta = 0$, which corresponds to the horizontal axis, we have that $\tau_l = y_l$ and $\tau_u = y_u$; all the data are censored, no transmission is allowed and all the sensors stay silent. To the other extreme, in the absence of censoring, $\beta = 1$ and the horizontal line representing $\beta$ has only one intersection with the curve $h(\tau)$, yielding $\tau_l = \tau_u$. For intermediate values of $\beta$, there always exists a single pair of thresholds $\tau_l \leq 1$ and $\tau_u \geq 1$ such that $h(\tau_l) = h(\tau_u)$. Furthermore, it is clear that $\tau_u(\beta)$ is a strictly decreasing function ranging from $y_u$ to 1, while $\tau_l(\beta)$ is strictly increasing that ranges from $y_l$ to 1.

Proof of Theorem 1. In view of the previous proved property
of the pair \((\tau_1, \tau_u)\), the function \(D(\beta)\) can be evaluated as
\[
D(\beta) = \int_{y_l}^{y_u} p_0(y) C(y) dy + \int_{\tau_u(\beta)}^{y_u} p_0(y) C(y) dy,
\]
whose derivative is
\[
\frac{dD(\beta)}{d\beta} = \frac{dD/d\tau_u}{d\beta/d\tau_u}.
\]
Now,
\[
\begin{align*}
\frac{dD}{d\tau_u} &= p_0(\tau_u) C(\tau_u) \frac{d\tau_1}{d\tau_u} - p_0(\tau_u) C(\tau_u), \\
\frac{d\beta}{d\tau_u} &= p_0(\tau_u) \frac{d\tau_1}{d\tau_u} - p_0(\tau_u),
\end{align*}
\]
By differentiating both sides of eq. (13), we see that the function \(\tau_1(\tau_u)\) has the further property
\[
\frac{d\tau_1}{d\tau_u} = \frac{g(\tau_1)}{g(\tau_u)}.
\]
where we just applied the definition of divergence per unit cost.

Now, the first maximum is obtained at \(\beta = 1/m\), which will give in general a value smaller than the true maximum \(D_a(m)\), that is
\[
D_a(m) \geq (1 - 1/m)^{m-1} D(1/m) / m.
\]

B. Results for the MAC case

Proof of Theorem 2. It is easy to upper bound \(D_a(m)\) as
\[
D_a(m) \leq m \max_{\beta \in [0,1]} [\beta(1-\beta)^{m-1}] \sup_{\beta \in (0,1)} \frac{D(\beta)}{\beta}.
\]

Now, the first maximum is obtained at \(\beta = 1/m\), giving
\[
D_a(m) \leq (1 - 1/m)^{m-1} D.
\]

REFERENCES


