Aldalahmeh *et al. EURASIP Journal on Advances in Signal Processing* (2016) 2016:5
DOI 10.1186/s13634-016-0303-9

EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

Optimal fusion rule for distributed detection in clustered wireless sensor networks

Sami A. Aldalahmeh[1*], Mounir Ghogho[2,3], Des McLernon[2] and Edmond Nurellari[2]

Abstract

We consider distributed detection in a clustered wireless sensor network (WSN) deployed randomly in a large field for the purpose of intrusion detection. The WSN is modeled by a homogeneous Poisson point process. The sensor nodes (SNs) compute local decisions about the intruder's presence and send them to the cluster heads (CHs). A stochastic geometry framework is employed to derive the optimal cluster-based fusion rule (OCR), which is a weighted average of the local decision sum of each cluster. Interestingly, this structure reduces the effect of false alarm on the detection performance. Moreover, a generalized likelihood ratio test (GLRT) for cluster-based fusion (GCR) is developed to handle the case of unknown intruder's parameters. Simulation results show that the OCR performance is close to the Chair-Varshney rule. In fact, the latter benchmark can be reached by forming more clusters in the network without increasing the SN deployment intensity. Simulation results also show that the GCR performs very closely to the OCR when the number of clusters is large enough. The performance is further improved when the SN deployment intensity is increased.

Keywords: Wireless sensor network, Cluster, Distributed detection, Fusion rule, Stochastic geometry

1 Introduction

A wireless sensor network (WSN) consists of a large number of geographically distributed low-cost sensor nodes (SNs) forming a network via wireless links. This structure enabled the instrumentation of WSNs in many applications [1]. Detecting an intruder in a monitored region of interest (ROI) is one of the most important applications of WSNs [2, 3]. The SNs monitor the ROI to detect abnormal phenomena, which might take the form of temperature, electromagnetic, or acoustic disturbances. Such physical signals are usually localized in space, i.e., the signal's power attenuates with the distance between the source and the sensor. The sensor nodes (SNs) sample the physical signal and then wirelessly communicate their data to a remote fusion center (FC), where the final decision about any intrusion is made. Due to bandwidth and power constraints, the data is often compressed to a single bit representing the local decision of the SN. When the ROI is very large, the WSN is divided into clusters to manage the large number of SNs needed to provide adequate coverage. In each cluster, the SNs send data to a cluster head (CH), which subsequently reports to the FC.

There is a large body of literature studying the problem of distributed detection and decision fusion for a single fusion center network configuration [4–6]. Chair and Varshney derived the optimum fusion rule in [7], which requires knowledge of local detection and false alarm probabilities for each SN. Niu and Varshney relaxed the latter requirement leading to the suboptimal counting rule (CR) [8]. The performance of the CR was investigated in [9]. However, the CR suffers from the problem of spurious detection in large WSN. This problem was tackled by using the scan statistic (SS) detector in [10] and [11]. In SS, a moving FC travels across the ROI and scans the SNs. This can be interpreted as sliding a window across the ROI, summing the number of positive local decisions, and continuously testing against a threshold. However, the SS rule is sequential in nature and hence incurs communication and delay penalties.

For a cluster-based WSN on the other hand, clustering algorithms for WSN [12] have been extensively studied in various contexts such as energy management [13] and routing [14]. Clustering and data aggregation in

*Correspondence: sami_dalahmah@ieee.org; s.aldalahmeh@zuj.edu.jo
[1] Al-Zaytoonah University of Jordan, Amman, Jordan
Full list of author information is available at the end of the article

WSNs have been surveyed in [15]. Power-constrained distributed estimation in WSNs was addressed in [16] where network communication was based on the amplify-and-forward scheme. The latter was also adopted in [17] where the optimum power allocation strategy was investigated. Quantized sensor observations were used in [18, 19] for distributed estimation in a clustered multi-hop WSN.

Decentralized detection in multi-level clustered WSNs has been considered in [20]. Each level of CHs uses a majority-like fusion rule to fuse the data from the level beneath it. The results in [20] (surprisingly) show that clustering decreases the detection performance. The effect of uniform and nonuniform clustering work was studied in [21]. In [22], the authors studied the performance of data fusion in a clustered Zigbee WSN implementation of [20]. The effect of communication errors on distributed detection in multi-hop clustered WSN was considered in [23] where it was shown that the optimal fusion rule is a weighted order statistic filter.

In this paper, we adopt the network configuration in [8] in which a vast WSN is divided into geographical regions managed by CHs. However, we assume that within each CH, the SNs send a single bit, representing their local decision, to the CH due to bandwidth and power constraints. The CHs then send the sums of the local decisions to the FC where the ultimate detection decision is made. We expand our previous work [24] using a stochastic geometry framework [25, 26] to derive the optimal cluster-based fusion rule (OCR). In contrast to [20], we show that clustering significantly improves the detection performance. In fact, the OCR is shown to have a performance very close to that of the optimal Chair-Varshney fusion rule (CVR) while it does not require the knowledge of the exact SNs locations unlike the CVR. Moreover, using stochastic geometry, we develop a generalized likelihood ratio test (GLRT) for the clustered-based fusion rule to handle the case of unknown intruder's parameters.

The paper is organized as follows. Section 2 presents models for the intruder, sensing, and communication. In Section 3, fusion rules for a single fusion point network are reviewed. The optimal fusion rule is presented in Section 4, which also contains the GLRT development. In Section 5, the simulation results are presented showing the performance of the proposed fusion rules. Finally, conclusions are given in Section 6.

2 System model

In this section, we present the models for sensing, the sensor network, and communication in the WSN. In addition, a stochastic geometry model is presented for the WSN.

2.1 Sensing and sensor network model

Consider a WSN deployed in a certain area, $\mathcal{A} \subset \mathbb{R}^2$ where $\mathcal{A}$ is assumed to be significantly large. The SNs are randomly dispersed in $\mathcal{A}$ according to a uniform distribution, i.e., the coordinate of the ith SN, $\mathbf{x}_i = (x_i, y_i)^T$, is a uniform random variable (RV) in $\mathcal{A}$. Also, the number of the SNs, N, is assumed to be a RV. The random characteristic of N can be justified by SN failure or battery exhaustion.

The WSN is tasked with the detection of any intruder entering the ROI. An intruder at location $\mathbf{x}_0 \in \mathcal{A}$ leaves a signature signal sensed by the SNs. Similar to [8, 11], this signature is assumed to decay with distance according to a power law. Thus, the intruder's parameters are given in the vector $\boldsymbol{\theta} = [P_0, \mathbf{x}_0]^T$, where P_0 is the intruder's signal power. The noise-free signal received at the ith SN has the following form:

$$a(\mathbf{x}_i) = \frac{\sqrt{P_0}}{\max(d_0, d_i)}, \tag{1}$$

where d_0 is the reference distance to the node's sensor and $d_i = \|\mathbf{x}_0 - \mathbf{x}_i\|$ is the Euclidean distance between the intruder and the ith SN. Note that the measured signal is saturated if the distance to the target is smaller than d_0. The above model can adequately describe acoustic or electromagnetic signals.

Each SN samples the environment to decide whether an intruder is present. The collected data at the ith SN under the null and alternative hypotheses, $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, takes the following form:

$$\mathcal{H}_1 : s(\mathbf{x}_i) = a(\mathbf{x}_i) + n(\mathbf{x}_i) \tag{2}$$

$$\mathcal{H}_0 : s(\mathbf{x}_i) = n(\mathbf{x}_i), \tag{3}$$

where $n(\mathbf{x}_i)$ is a white Gaussian noise at the SN located at $\mathbf{x}_i$ with zero mean and variance σ_s^2. The noise is assumed to be identically and independently distributed over all the SNs. The sensing signal-to-noise ratio (SNR) is defined as

$$\mathrm{SNR}_s = \frac{P_0}{\sigma_s^2}. \tag{4}$$

Each SN computes its binary local decision, $I(\mathbf{x}_i) = \{0, 1\}$, by comparing the collected data with a local decision threshold τ, i.e.,

$$I(\mathbf{x}_i) = \begin{cases} 1, & s(\mathbf{x}_i) \geq \tau \\ 0, & s(\mathbf{x}_i) < \tau \end{cases}. \tag{5}$$

Here, τ is the same for all SNs. Therefore, the local probabilities of detection and false alarm are given by

$$P_d(\mathbf{x}_i) = Q\left(\frac{\tau - a(\mathbf{x}_i)}{\sigma_s}\right) \tag{6}$$

$$P_{fa} = Q\left(\frac{\tau}{\sigma_s}\right) \tag{7}$$

where $Q(\cdot)$ is the Gaussian Q-function given by

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt. \tag{8}$$

Note, however, that the probability of detection in (6) depends on the target parameters P_0 and $\mathbf{x}_0$ through (1).

2.2 Stochastic geometry model

The WSN defined above can be elegantly modeled using stochastic geometry [25], which has recently attracted interest in the modeling of wireless networks [27, 28] and cognitive radios [29].

We model the spatial distribution of the SNs as a Poisson point process (PPP) $\Phi = \{\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_N\}$ in $\mathcal{A}$. This implies that the $\mathbf{x}_i$'s $\in \Phi$ are uniform RVs and their number $N = |\Phi|$ is a Poisson RV, i.e., $N \sim \text{Pois}(\lambda|\mathcal{A}|)$, where λ is the average number of points (SNs) in a unit area (deployment intensity) and $|\mathcal{A}|$ is the area of $\mathcal{A}$. Φ is assumed to be simple (no two points occupy the same location) and stationary in space, i.e., its statistical properties do not change if Φ is shifted. A PPP is called homogeneous if the intensity, λ, is independent of the location $\mathbf{x}$. Otherwise, it is called inhomogeneous.

The thinning of a PPP is the process of removing points from the original PPP that do not adhere to some rule, and hence, a point is removed from the PPP with some probability. Thinning can be independent (p-thinning), i.e., the thinning probability does not depend on the location of the point under consideration, or it can be dependent, i.e., the thinning probability depends on the point's location.

Thinning is used here to model the local detection operation. If Φ is thinned to produce Φ_d, the PPP of detecting SNs

$$\Phi_d = \{\mathbf{x}_i \in \Phi : I(\mathbf{x}_i) = 1\} \tag{9}$$

The properties of Φ_d are used to derive the optimal fusion rule as given in Section 4.

2.3 Communication model

Due to the vastness of the ROI, the WSN is geographically divided into M disjoint zones: $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_M$, where $\mathcal{C}_m \in \mathcal{A}$ for $m = 1, \cdots, M$. Each zone is managed by a CH located at $\mathbf{x}_m \notin \Phi$. The number of clusters is fixed, and their locations are also fixed and known to the WSN. SNs located at $\mathbf{x}_i \in \mathcal{C}_m$ send their decisions to the mth CH. The CHs in turn report back to the FC.

Due to cost and bandwidth constraints, SNs use on-off keying (OOK) to transmit their binary local decisions to the CH. Only the SNs making positive local decisions report to the CHs. These SNs are assumed to be synchronized to the same time slot. Furthermore, a power control strategy is assumed to be used at the SNs in order to ensure that the powers of the signals received from the SNs at the CH are all equal to the same desired value. This power level is chosen such that the effect of the channel noise is negligible.

Each CH then communicates with the FC over wireless channel that is less restricted in bandwidth. Moreover, the CH encodes its data for protection against errors. This is justified by the argument that the network has only $M \ll N$ CHs, and so it can afford having more sophistication in the CHs.

3 Fusion rules for single cluster WSNs

In this section, we review fusion rules for distributed detection in a cluster WSN.

In this configuration, all SNs in the network report to a single CH that acts as the FC. The optimal hard decision fusion rule in this case is CVR, which is given by [7]

$$\Lambda_{\text{CVR}} = \sum_{i=1}^{N} I(\mathbf{x}_i) \log\left(\frac{P_d(\mathbf{x}_i)}{P_{fa}}\right) + (1 - I(\mathbf{x}_i)) \log\left(\frac{1 - P_d(\mathbf{x}_i)}{1 - P_{fa}}\right). \tag{10}$$

This rule requires the complete knowledge of the intruder's parameters in addition to both the number of SNs and their locations. Such conditions are difficult to attain in large WSNs.

Relaxing the above conditions, Niu and Varshney proposed the following suboptimal counting rule [8]:

$$\Lambda_{\text{CR}} = \sum_{i=1}^{N} I(\mathbf{x}_i). \tag{11}$$

As can be seen in (11), the CR does not require any information about the target or the SNs locations.

However, for a large ROI, the problem of spurious detection becomes more prevalent as shown in Fig. 1. The intruder is located in the north-east cluster, in which the number of detecting SNs is relatively large, whereas the number of detecting SNs in the south-west cluster is small. These positive decisions are mainly due to the sensing noise. This problem was tackled by using the scan statistic (SS) detector proposed in [10]. The SS test statistic is given by

$$\Lambda_{\text{SS}} = \max_i \left(\frac{\lambda_1^{\text{SS}}}{\lambda_0^{\text{SS}}}\right)^{Z_i}, \quad i = 1, \cdots, L, \tag{12}$$

where L is the number of sliding window iterations, Z_i is the number of positive decisions in the ith *window slide iteration*, and λ_0^{SS} and λ_1^{SS} are the mean number of detecting SNs in a typical window under the $\mathcal{H}_0$ and $\mathcal{H}_1$ hypotheses, respectively.

The Bayesian form of the SS is given by [11]

$$\Lambda_{\text{B-SS}} = \sum_{i=1}^{L} \left(\frac{\lambda_1^{\text{SS}}}{\lambda_0^{\text{SS}}}\right)^{Z_i}. \tag{13}$$

The SS was shown to outperform the CR for the case where the WSN has a high node intensity [11].

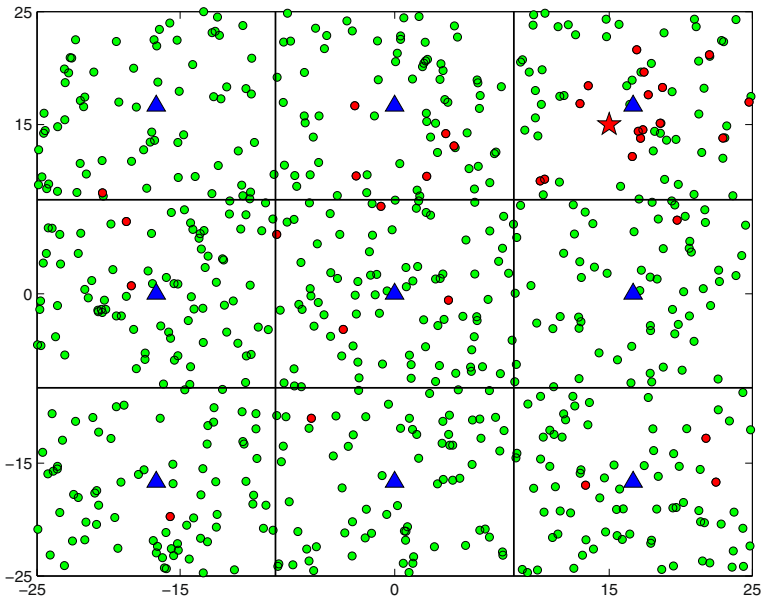

Fig. 1 Poisson field of sensor nodes. *Pentagram*: intruder, *green circle*: SN; *red circle*: detecting SN; *blue triangle*: CH. The system parameters are $\lambda = 0.3$, $P_0 = 50$, $d_0 = 1$, $\sigma_s^2 = 1$, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (15, 15)^T$

4 Fusion rules in clustered WSNs

In this section, we present the fusions rules for clustered WSNs in the CH and FC levels. For the purpose of motivation, the majority-like fusion rule [20] is presented first. Then, we propose the optimal clustered-based fusion rule followed by the GLRT development.

4.1 Decision fusion in the cluster heads

SNs with positive decisions send their local decision to the related CH, which acts as a fusion point for SNs in the cluster as shown in Fig. 2. The fusion rule adopted in each cluster is the CR. In addition to its simplicity, this handles the situation in which information on the SNs is lacking, which is the case in random networks.

Accordingly, the fused data from the mth cluster, Λ_m, takes the following form:

$$\Lambda_m = \sum_{\mathbf{x}_i \in \mathcal{C}_m} I(\mathbf{x}_i). \tag{14}$$

4.2 Majority-like fusion rule

We consider the majority-like fusion rule (MFR) with a two-level network, i.e., one level of CHs reporting to a FC which is the second level. The mth CH uses a majority-like rule to produce the CH's decisions $\tilde{I}_m$ as follows;

$$\tilde{I}_m = \begin{cases} 1, & \Lambda_m \geq k_1 \\ 0, & \Lambda_m < k_1 \end{cases}, \tag{15}$$

where $k_1 = \lceil |\Phi_m|/2 \rceil + 1$ is the first level majority rule threshold and $|\Phi_m|$ is the number of SNs in the mth cluster. The $\tilde{I}_m$'s can be thought of as the one-bit compression of the Λ_m.

However, in random networks, the number of SNs in each cluster is not known. Moreover, the source signal is spatially localized leading to a different number of detecting SNs in each cluster. So choosing k_1 as defined previously negatively affects the performance. The $\tilde{I}_m$'s are then sent to the FC for another level of majority rule fusion as described next

$$\Gamma = \sum_{m=1}^{M} \tilde{I}_m \tag{16}$$

$$I_g = \begin{cases} 1, & \Gamma \geq k_2 \\ 0, & \Gamma < k_2 \end{cases}, \tag{17}$$

where $k_2 = \lceil M/2 \rceil + 1$ is the second level majority rule threshold and I_g is the global decision about the intruder's presence. Note that the MFR virtually uses the CR in the CH and FC levels.

4.3 Optimal cluster-based fusion rule

In contrast to MFR, we investigate the optimal scheme to fuse the CHs data, $\{\Lambda_m\}_{m=1}^M$. Employing the Neaman-Pearson criterion ([30], Chap. 3), the log-likelihood ratio (LLR) test is expressed as

$$\Lambda_{\text{OCR}} = \sum_{m=1}^{M} \log \left(\frac{p\left(\Lambda_m; \mathcal{H}_1\right)}{p\left(\Lambda_m; \mathcal{H}_0\right)} \right), \tag{18}$$

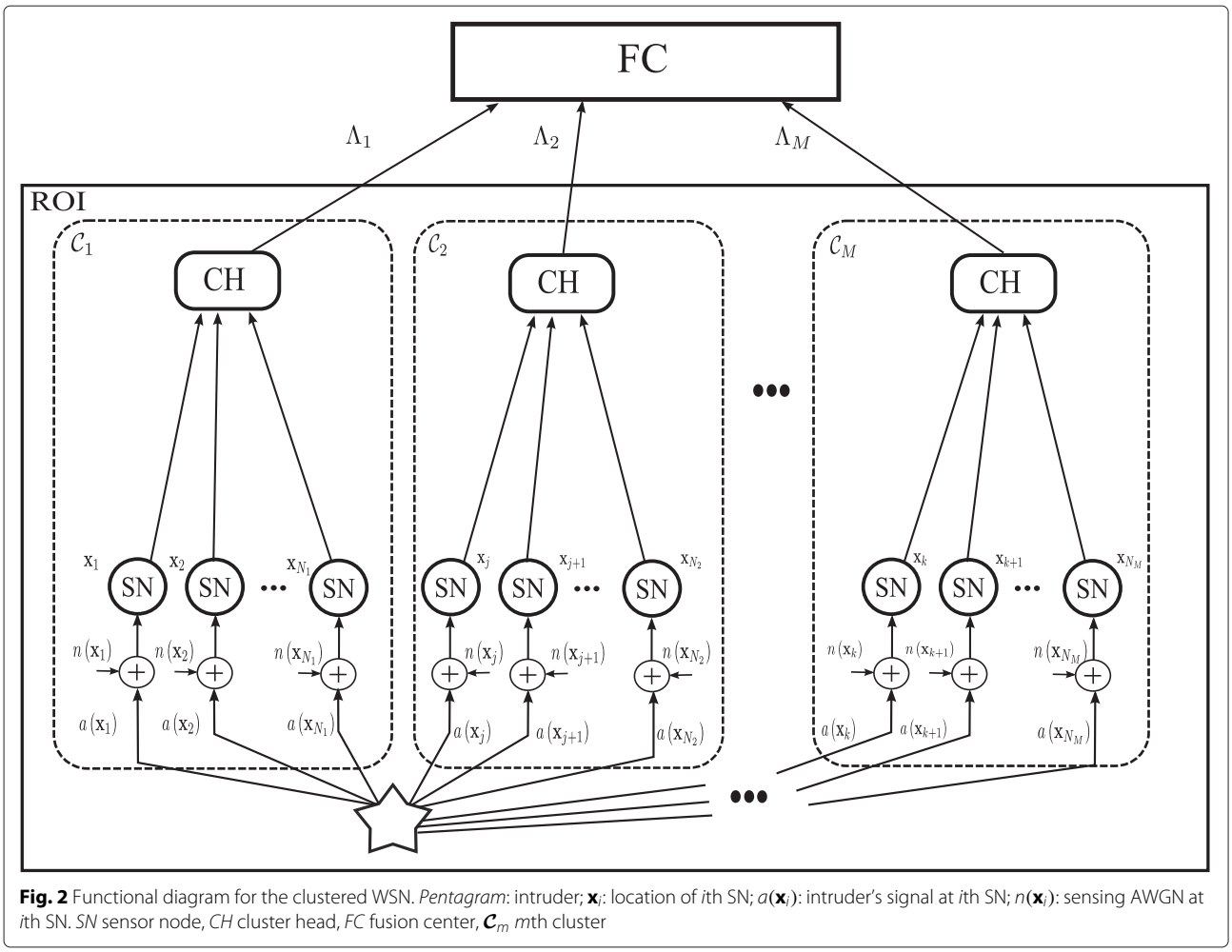

Fig. 2 Functional diagram for the clustered WSN. *Pentagram*: intruder; $\mathbf{x}_i$: location of *i*th SN; $a(\mathbf{x}_i)$: intruder's signal at *i*th SN; $n(\mathbf{x}_i)$: sensing AWGN at *i*th SN. *SN* sensor node, *CH* cluster head, *FC* fusion center, $\mathcal{C}_m$ *m*th cluster

where $p(\Lambda_m; \mathcal{H}_j)$ is the likelihood of Λ_m under hypothesis $\mathcal{H}_j$ for $j = 0, 1$.

To evaluate the LLR test, we investigate the properties of the detecting point process Φ_d in (9). The statistics of Φ_d under $\mathcal{H}_0$ are given by the following lemma.

Lemma 1. *The detecting SN point process* Φ_d *defined in* (9) *under* $\mathcal{H}_0$ *is a homogeneous PPP with intensity of* λP_{fa}.

Proof. See Appendix A. □

Remark 1. *It can be noted that if* $\mathcal{A}$ *is large, the number of detecting SNs is also large. Thus, the performance of simple rules such as the CR will suffer degradation and sophisticated rules such as the CVR will burden the network with large communication load. This motivates the use of clusters to divide the ROI into manageable areas with relatively low number of false alarms and communication burden.*

Similarly, the statistics of Φ_d under $\mathcal{H}_1$ are given in the following lemma.

Lemma 2. *The detecting SN point process* Φ_d *defined in* (9) *under* $\mathcal{H}_1$ *is an inhomogeneous PPP with intensity* $\lambda P_d(\mathbf{x})$.

Proof. See Appendix B. □

The above lemma implies that as the distance from the intruder increases the mean number of detecting SNs decreases due to the nature of the detection probability P_d defined in (6).

Remark 2. *The detecting intensity of SNs decreases gradually as we move away from the intruder until it reaches the value of* λP_{fa}, *implying that the intruder's signal has no effect at this point. This fact also motivates the use of clusters since the detecting SNs are much more likely to be close to the intruder.*

From the above lemmas, the distribution of the total number of detecting SNs in the network can be directly inferred as stated in the following corollary.

Corollary 1. *Let the total number of detecting SNs be*

$$\Lambda = \sum_{\mathbf{x}_i \in \Phi_d} \mathbf{1}(\mathbf{x}_i). \tag{19}$$

Then, Λ is Poisson distribution with

$$\Lambda \sim \begin{cases} \text{Pois}\left(\lambda_0\right), & \mathcal{H}_0 \\ \text{Pois}\left(\lambda_1\right), & \mathcal{H}_1 \end{cases}, \tag{20}$$

where λ_0 and λ_1 are the mean numbers of detecting SNs under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, and are given by

$$\lambda_0 = \lambda P_{fa} |\mathcal{A}| \tag{21}$$

$$\lambda_1 = \lambda \int_{\mathcal{A}} P_d(\mathbf{x}) d\mathbf{x}. \tag{22}$$

Proof. See Appendix B. □

Consequently, the distribution of the CR test statistic is directly given by (20) as it was shown in [24]. Furthermore, the distribution of Λ_m follows directly from the Poisson property of Φ_d as stated by the following corollary.

Corollary 2. *The distribution of Λ_m is*

$$\Lambda_m \sim \begin{cases} \text{Pois}\left(\lambda_{0,m}\right), & \mathcal{H}_0 \\ \text{Pois}\left(\lambda_{1,m}\right), & \mathcal{H}_1 \end{cases}, \tag{23}$$

where $\lambda_{0,m}$ and $\lambda_{1,m}$ are mean numbers of detecting SNs in the mth cluster under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, and are given by

$$\lambda_{0,m} = \lambda P_{fa} |\mathcal{C}_m| \tag{24}$$

$$\lambda_{1,m} = \lambda \int_{\mathcal{C}_m} P_d(\mathbf{x}) d\mathbf{x}. \tag{25}$$

Proof. Since Λ is a Poisson RV over $\mathcal{A}$ and the Λ_m's are defined in (14) over the $\mathcal{C}_m$'s that are disjoint areas in $\mathcal{A}$, then Λ_m is a Poisson RV over $\mathcal{C}_m$. □

Note that if all the $\mathcal{C}_m$'s have the same area, say $|\mathcal{C}|$, then $\lambda_{0,m} = \lambda P_{fa} |\mathcal{C}|$ for all $m = 1, \cdots, M$. Hence, under $\mathcal{H}_0$, all the Λ_m's have the same distribution under $\mathcal{H}_0$.

With this information at hand, the OCR defined earlier in (18) can be written as

$$\begin{aligned} \Lambda_{\text{OCR}} &= \sum_{m=1}^{M} \log \left(\frac{e^{-\lambda_{1,m}} \left(\lambda_{1,m}^{\Lambda_m} / \Lambda_m! \right)}{e^{-\lambda_{0,m}} \left(\lambda_{0,m}^{\Lambda_m} / \Lambda_m! \right)} \right) \\ &= \sum_{m=1}^{M} \Lambda_m \log \left(\frac{\lambda_{1,m}}{\lambda_{0,m}} \right), \end{aligned} \tag{26}$$

where the constant term above is ignored in the second line of the equation.

Remark 3. *Note, however, that $\lambda_{1,m}$ is a scaled spatial average of the detection probability in* (6)*, which is the direct result of applying Campbell's theorem ([26], Chap. 2) in* (33)*. This relieves the OCR from knowing the SNs' positions, in contrast to the CVR. Nonetheless, finding the $\lambda_{1,m}$'s requires knowing the intruder's parameters, P_0 and x_0, a topic that will be discussed later in Subsection 4.4.*

Thus, the OCR is a weighted sum of the number of positive decisions in each cluster. Clusters with larger detecting SNs means, $\lambda_{1,m}$, are given more weight since it is expected that the intruder is in their vicinity. On the other hand, clusters with smaller detecting SNs means are given less weight since the intruder is expected to be far away and hence the detecting SNs in such clusters are due to false alarms. In this sense, the problem of spurious detection is adequately handled.

4.4 Generalized likelihood ratio test for clustered-based fusion

As mentioned earlier, the OCR requires the knowledge of the $\lambda_{1,m}$'s, which are implicitly dependent on the intruder's parameters, i.e., $\boldsymbol{\theta} = (P_0, \mathbf{x}_0)^T$. Unfortunately, such information is not available in realistic scenarios since the intruder is not cooperative with the network. In this case, we resort to the GLRT ([30], Chap. 7) method, which consists of replacing the unknown parameters in the LLR by their maximum likelihood estimates.

The data used to estimate $\boldsymbol{\theta}$ is the set $\{\Lambda_m\}_{m=1}^{M}$ available at the FC. The GLRT for the clustered-based fusion, termed here (GCR), is given by

$$\Lambda_{\text{GCR}} = \max_{\boldsymbol{\theta} \in \boldsymbol{\theta}} \sum_{m=1}^{M} \Lambda_m \log \left(\frac{\lambda_{1,m}(\boldsymbol{\theta})}{\lambda_{0,m}} \right), \tag{27}$$

where $\boldsymbol{\theta} \subset \mathbb{R}^3$ is the space of all $\boldsymbol{\theta}$ values.

Note that the dependence of $\lambda_{1,m}$ on $\boldsymbol{\theta}$ is via the detection probability defined in (6). The GLRT in (27) can be interpreted as finding the optimal set of weights that maximize the weighted average of Λ_m's.

However, problem (27) is a nonlinear three-dimensional optimization problem, which is usually solved via numerical techniques. To reduce the complexity, the search space is a restricted version of the original, Θ. In particular, the search space for the target's position is restricted to the clusters centroids, $\mathbf{x}_{c,m}$, given by

$$\mathbf{x}_{c,m} = \frac{1}{|\mathcal{C}_m|} \int_{\mathcal{C}_m} \mathbf{x}\, d\mathbf{x}, \tag{28}$$

for $m = 1, \cdots, M$. Although, the restricted search space is significantly smaller than the original, the corresponding

Table 1 Fusion rules list

Abbreviation	Equation	Fusion rule
CVR	(10)	Chair-Varshney
CR	(11)	Counting
SS	(12)	Scan statistic
B-SS	(13)	Bayesian SS
MFR	(17)	Majority-like
OCR	(26)	Optimal clustered-based
GCR	(27)	GLRT clustered-based

results as shown in Section 5 are very close to the optimal CVR.

5 Simulation results

We simulate a WSN deployed in a 50×50 ROI. The intruder's power is $P_0 = 1$. The sensing SNR is set to 0 dB. The SNs have a reference distance of $d_0 = 1$ units with a local probability of false alarm of 10^{-2}. We simulate the fusion rules listed in Table 1 and compare them in using the above setting. The proposed GCR is implemented via a grid search, as stated earlier, on a restricted search space as described next. The values considered for the power P_0 are obtained by linearly discretizing the interval $[0.1, 1]$; ten values used for the simulations. The discretization of x_0 is done by dividing the ROI into adjacent squares girds with side length of A/N each, where A is the ROI side length ($A = 50$ in our simulation setup) and N is the number of clusters. The centers of those squares in addition to the discretized power values are used to form the restricted search space.

First, we validate Corollaries 1 and 2 by simulation. Figure 3 shows the results of a Monte Carlo simulation with 10^5 runs to produce the simulated and theoretical distribution of Λ defined in (19) or that of Λ_{CR} in (11). The exact Poisson distribution given in Corollary 1 fits the simulation perfectly for both $\mathcal{H}_0$ and $\mathcal{H}_1$. For the same setup, the WSN is divided into four squared-shaped clusters and the distributions of the Λ_m's in the four clusters are shown in Figs. 4 and 5. Again, the theoretical Poisson distributions given in Corollary 2 fit the simulation accurately. Note, however, that under $\mathcal{H}_0$ all Λ_m's have the same distribution. Under $\mathcal{H}_1$ on the other hand, Λ_3 differs since the intruder is located in the region monitored by the third cluster. Λ_1, Λ_2, and Λ_4 have a distribution similar to the $\mathcal{H}_0$ case since the intruder is not sensed by SNs in the those clusters.

Figure 6 show the ROC diagrams for the fusion rules mentioned in Table 1 for different values of λ, obtained by 10^4 Monte Carlo runs. The OCR uses 25 square-shaped clusters to cover the ROI. The same number of clusters is used for the MFR. The decision threshold for all the

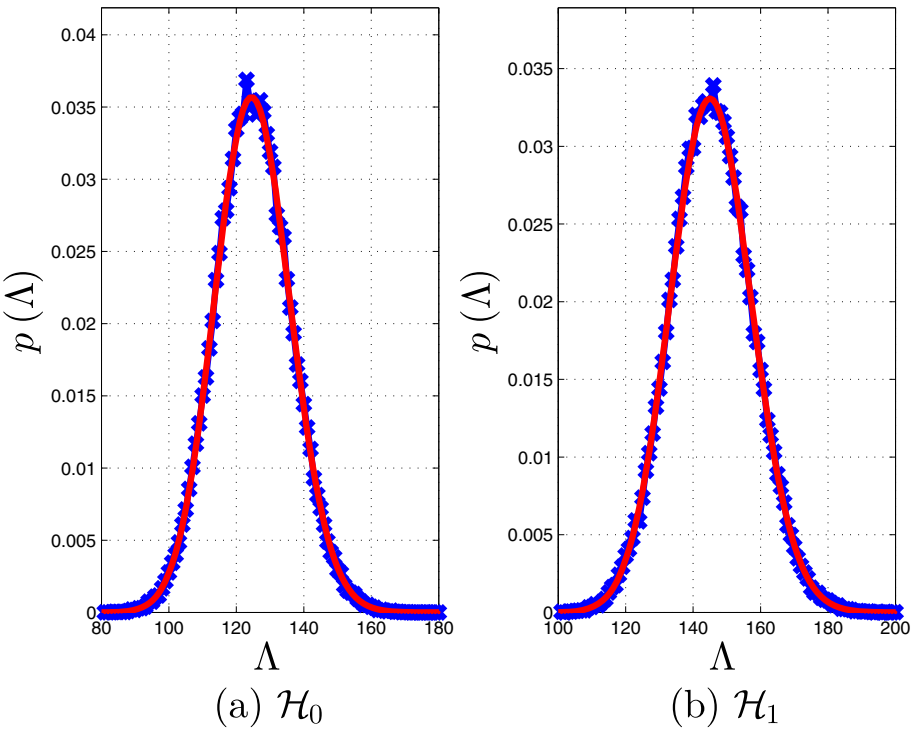

Fig. 3 Distribution of Λ (**a**, **b**). The system parameters are $\lambda = 5$, $d_0 = 1$, $\mathrm{SNR}_s = 0$ dB, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (20, 20)^T$. *x* for simulation distribution and *solid line* for Poisson distribution in Corollary 1

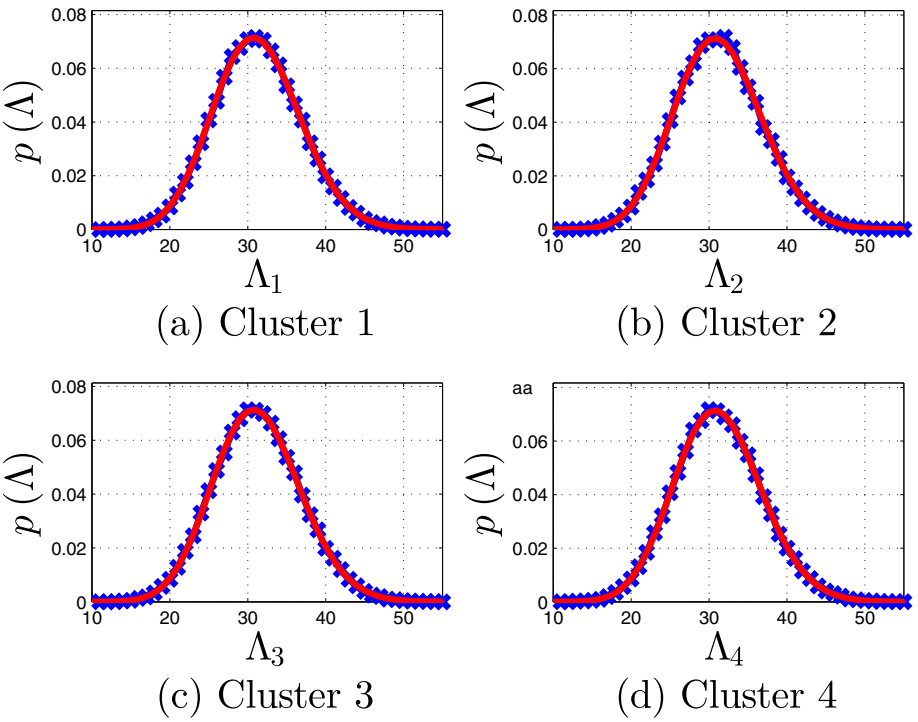

Fig. 4 Distribution of CH data, Λ_m, under $\mathcal{H}_0$ for $\lambda = 5$ and number of clusters $M = 4$ (**a**–**d**). The system parameters are $\lambda = 5$, $d_0 = 1$, $\text{SNR}_s = 0$ dB, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (20, 20)^T$. *x* for simulated distribution and *solid line* for Poisson distribution in Corollary 2

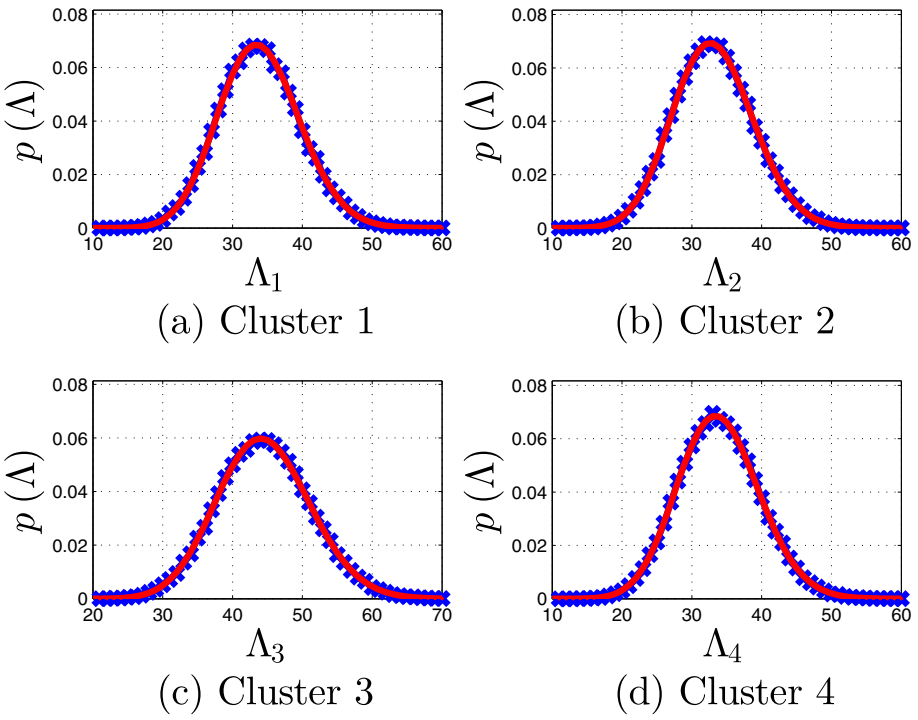

Fig. 5 Distribution of CH data, Λ_m, under $\mathcal{H}_1$ for $\lambda = 5$ and number of clusters $M = 4$ (**a**–**d**). The system parameters are $\lambda = 5$, $d_0 = 1$, $\text{SNR}_s = 0$dB, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (20, 20)^T$. *x* for simulated distribution and *solid line* for Poisson distribution in Corollary 2

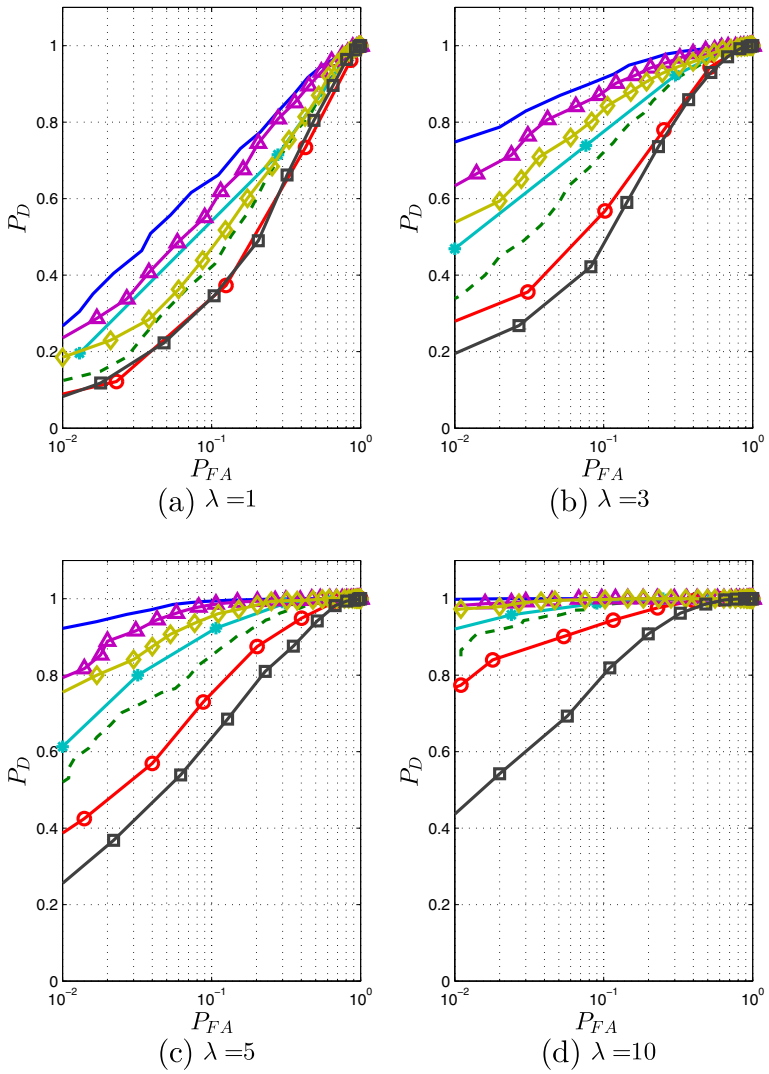

Fig. 6 ROC diagrams for a network with 25 clusters (**a**–**d**). The system parameters are $d_0 = 1$, $\text{SNR}_s = 0\text{dB}$, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (0, 0)^T$. CVR *solid line*, CR *dashed line*, OCR *triangle*, GCR *diamond*, MFR *square*, SS *asterisk*, B-SS *circle*

CHs in the MFR are the same and are set according to Corollary 2 to provide a cluster level false alarm rate of 0.1 approximately. To make the comparison fair, the SS and the B-SS use a window with the same size as the clusters used in the OCR. The OCR shows superior performance compared to the rest of the rules. In fact, as λ increases, the OCR approaches the optimal performance of the benchmark CVR. The GCR follows a similar trend as the OCR, in which it can be observed that the GCR rapidly approaches the OCR as λ increases and consequently it performs better than the SS, B-SS, CR, and the MFR. The SS algorithms show better performance when compared to the CR, which shows a relatively slow improvement as λ increases. The MFR performs the worst among all rules, this is due to utilizing the least amount of information when compared to the other rules.

Figure 7 illustrates the effect of increasing M, the number of clusters, on the performance of the fusion rules.[1] It is noted that when the number of clusters is small, the OCR resembles the CR in performance. This result is intuitive since the limit case of a single cluster is equivalent to the CR. The SS algorithms perform better because they use more information for fusion. However, as M increases, the OCR and GCR outperform the rest of the rules and ultimately reach the benchmark performance of the CVR. This behavior can be explained by the fact that as the number of clusters increases, the detecting SNs due to the intruder's presence are contained in clusters that are given large weights. On the other hand, clusters containing the spurious detection are given small weights, hence improving the detection performance.

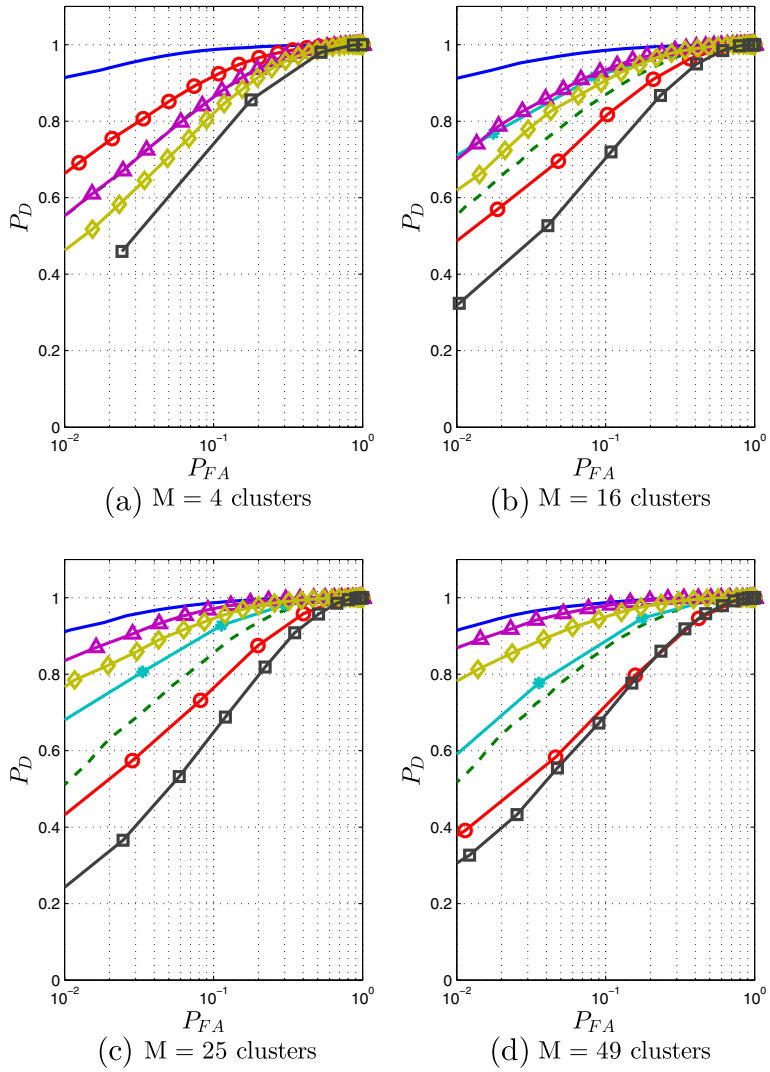

Fig. 7 ROC diagrams for a network with $\lambda = 5$ (**a**–**d**). The system parameters are $d_0 = 1$, $\text{SNR}_s = 0$ dB, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (0, 0)^T$. CVR *solid line*, CR *dashed line*, OCR *triangle*, GCR *diamond*, MFR *square*, SS *asterisk*, B-SS *circle*

6 Conclusions

We have studied fusion rules for distributed detection in random clustered WSNs. In each cluster, the CH collects the local decisions of the SNs and sends the sum to the FC. Using stochastic geometry, we derived the OCR, which is the weighted average of the sums of local decisions at each cluster. The weights are shown to depend on the mean number of detecting SNs under the null and alternative hypotheses. In contrast to the optimal Chair-Varshney rule, the OCR does not require the locations of the SNs to be known. Furthermore, a reduced-complexity GLRT for GCR is developed to handle the case of unknown intruder's parameters. Simulation results have shown that the performance of the OCR approaches that of the Chair-Varshney rule. Results also showed that as the number of clusters increases, the performance rapidly reaches the Chair-Varshney benchmark for fixed SNs deployment intensity. In other words, optimal detection can be achieved by forming more clusters in the network, in contrast to adding more sensor nodes to it. Finally, the performance of the GCR was shown to approach that of the OCR when the number of clusters is large enough. PAUSE

Endnote

[1]The B-SS is not shown in the case of $M = 4$ due to a severely bad performance.

Appendix A

Define the following marked PPP (MPPP):

$$\Phi_m = \{(\mathbf{x}_i, s(\mathbf{x}_i)) : \mathbf{x}_i \in \Phi, s \in \mathcal{S}\} \tag{29}$$

where the marks are chosen to be the collected data $s(\mathbf{x}_i)$ with the mark space $\mathcal{S}$. Construct the detecting PP Φ_d by thinning Φ_m. Under $\mathcal{H}_0$, however, the probability of $\mathbf{x}_i \in \Phi_d$ is

$$\begin{aligned}\mathbb{P}(\mathbf{x}_i \in \Phi_d) &= \mathbb{P}(I(\mathbf{x}_i) = 1; \mathcal{H}_0) \\ &= \mathbb{P}(s(\mathbf{x}_i) > \tau; \mathcal{H}_0) = P_{fa}\end{aligned} \tag{30}$$

which is constant across $\mathcal{A}$, and hence the thinning probability is also constant. Therefore, the thinned Φ_d is a homogeneous PPP with intensity given by λP_{fa}.

Appendix B

Define the detecting PP $\Phi_d = \{\mathbf{x}_i \in \Phi_m : s(\mathbf{x}_i) > \tau\}$. The former is obtained by thinning the MPPP Φ_m defined in (29) according to the probability

$$\begin{aligned}\mathbb{P}(\mathbf{x}_i \in \Phi_d) &= \mathbb{P}(I(\mathbf{x}_i) = 1; \mathcal{H}_1) \\ &= \mathbb{P}(s(\mathbf{x}_i) > \tau; \mathcal{H}_1) = P_d(\mathbf{x}_i).\end{aligned} \tag{31}$$

Note that the thinning probability depends on the intruder's parameters as mentioned earlier. Also, the thinning probability depends on $\mathbf{x}_i$ and so results in *dependent thinning*. Dependent thinning in turn produces an inhomogeneous PPP. Under $\mathcal{H}_1$, the mean of the total number of detecting SNs is given by

$$\begin{aligned}\lambda_1 &= \mathbb{E}\left[\sum_{\mathbf{x}_i \in \Phi_d} \mathbf{1}(\mathbf{x}_i)\right] \\ &= \mathbb{E}\left[\sum_{\mathbf{x}_i \in \Phi'_m} \mathbf{1}(s(\mathbf{x}_i) > \tau)\right],\end{aligned} \tag{32}$$

where $\mathbf{1}(A)$ is the indicator function for event A. Applying Campbell's theorem to find the above mean yields

$$\begin{aligned}\lambda_1 &= \lambda \int_{\mathcal{A}} \int_0^{\infty} \mathbf{1}(s(\mathbf{x}) > \tau; \mathcal{H}_1)\, dP(s) dx \\ &= \lambda \int_{\mathcal{A}} \mathbb{P}(s(\mathbf{x}) > \tau; \mathcal{H}_1)\, dx \\ &= \lambda \int_{\mathcal{A}} P_d(\mathbf{x}) dx,\end{aligned} \tag{33}$$

where $\mathbb{P}(A)$ is the probability of event A and $P(s)$ is the cumulative distribution function of the mark variable s.

Competing interests
The authors declare that they have no competing interests.

Author details
[1] Al-Zaytoonah University of Jordan, Amman, Jordan. [2] University of Leeds, Leeds, UK. [3] International University of Rabbat, Rabbat, Morocco.

Received: 8 August 2015 Accepted: 4 January 2016
Published online: 13 January 2016

References

1. C-Y Chong, SP Kumar, Sensor networks: evolution, opportunities, and challenges. Proc. IEEE. **91**(8), 1247–1256 (2003)
2. P Chen, O Songhwai, M Manzo, B Sinopoli, C Sharp, K Whitehouse, O Tolle, J Jaein, P Dutta, J Hui, S Schaffert, K Sukun, J Taneja, B Zhu, T Roosta, M Howard, D Culler, S Sastry, in *Robotics and Automation, 2006. ICRA 2006. Proceedings 2006 IEEE International Conference on*. Instrumenting wireless sensor networks for real-time surveillance, (2006), pp. 15–19
3. A Arora, P Dutta, S Bapat, V Kulathumani, H Zhang, V Naik, V Mittal, H Cao, M Demirbas, M Gouda, *et al*, A line in the sand: a wireless sensor network for target detection, classification, and tracking. Comput. Netw. **46**(5), 605–634 (2004)
4. PK Varshney, *Distributed Detection and Data Fusion*, 1st edn. (Springer, Secaucus, NJ, USA, 1996)
5. R Viswanathan, PK Varshney, Distributed detection with multiple sensors I. Fundamentals. Proc. IEEE. **85**(1), 54–63 (1997)
6. RS Blum, SA Kassam, HV Poor, Distributed detection with multiple sensors II. Advanced topics. Proc. IEEE. **85**(1), 64–79 (1997)
7. Z Chair, PK Varshney, Optimal data fusion in multiple sensor detection systems. IEEE Trans. Aerospace Electron. Syst. **AES-22**(1), 98–101 (1986)
8. R Niu, PK Varshney, Distributed detection and fusion in a large wireless sensor network of random size. EURASIP J. Wireless Commun. Netw. **2005**(4), 462–472 (2005)
9. R Niu, PK Varshney, Performance analysis of distributed detection in a random sensor field. Signal Process. IEEE Trans. **56**(1), 339–349 (2008)
10. M Guerriero, P Willett, J Glaz, Distributed target detection in sensor networks using scan statistics. Signal Process. IEEE Trans. **57**(7), 2629–2639 (2009)
11. M Guerriero, L Svensson, P Willett, Bayesian data fusion for distributed target detection in sensor networks. Signal Process. IEEE Trans. **58**(6), 3417–3421 (2010)
12. AA Abbasi, M Younis, A survey on clustering algorithms for wireless sensor networks. Comput. Commun. **30**(14), 2826–2841 (2007)
13. M Younis, M Youssef, K Arisha, Energy-aware management for cluster-based sensor networks. Comput. Netw. **43**(5), 649–668 (2003)
14. K Akkaya, M Younis, A survey on routing protocols for wireless sensor networks. Ad Hoc Netw. **3**(3), 325–349 (2005)
15. R Rajagopalan, PK Varshney, in *Communications Surveys & Tutorials, IEEE*. Data-aggregation techniques in sensor networks: A survey, vol. 8, (2006), pp. 48–63. Fourth Quarter
16. MH Chaudhary, L Vandendorpe, Performance of power-constrained estimation in hierarchical wireless sensor networks. Signal Process. IEEE Trans. **61**(3), 724–739 (2013)
17. J Fang, H Li, Power constrained distributed estimation with cluster-based sensor collaboration. Wireless Commun. IEEE Trans. **8**(7), 3822–3832 (2009)
18. Q Tian, EJ Coyle, in *Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings. 2006 IEEE International Conference on*. Optimal distributed estimation in clustered sensor networks, vol. 4, (2006), pp. 14–19
19. X Sun, EJ Coyle, Quantization, channel compensation, and optimal energy allocation for estimation in sensor networks. ACM Trans. Sen. Netw. **8**(2), 15–11525 (2012)
20. G Ferrari, M Martalo, R Pagliari, Decentralized detection in clustered sensor networks. Aerospace Electron. Syst. IEEE Trans. **47**(2), 959–973 (2011)
21. M Martalo, G Ferrari, A simple information-theoretic analysis of clustered sensor networks with decentralized detection. Commun. Lett. IEEE. **14**(6), 560–562 (2010)
22. P Medagliani, M Martalò, G Ferrari, Clustered Zigbee networks with data fusion: characterization and performance analysis. Ad Hoc Netw. **9**(7), 1083–1103 (2011)
23. Q Tian, EJ Coyle, Optimal distributed detection in clustered wireless sensor networks. Signal Process. IEEE Trans. **55**(7), 3892–3904 (2007)
24. SA Aldalahmeh, M Ghogho, A Swami, in *2011 IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC 2011)*. Distributed detection of an unknown target in clustered wireless sensor networks, (San Francisco, USA, 2011)
25. D Stoyan, *Stochastic Geometry and Its Applications*. (Wiley, Chichester New York, 1995)

26. R Streit, *Poisson Point Processes Imaging, Tracking, and Sensing*. (Springer, New York, 2010)
27. M Haenggi, JG Andrews, F Baccelli, O Dousse, M Franceschetti, Stochastic geometry and random graphs for the analysis and design of wireless networks. IEEE J. Selected Areas Commun. **27**(7), 1029–1046 (2009)
28. JG Andrews, RK Ganti, M Haenggi, N Jindal, S Weber, A primer on spatial modeling and analysis in wireless networks. Commun. Mag. IEEE. **48**(11), 156–163 (2010)
29. H ElSawy, E Hossain, M Haenggi, Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: a survey. Commun. Surv. Tutor. IEEE. **15**(3), 996–1019 (2013)
30. SM Kay, *Fundamentals of Statistical Signal Processing, Volume 2: Detection Theory*. (Prentice Hall, Englewood Cliffs, N.J, 1998)