Reliable distributed detection in multi-hop clustered wireless sensor networks

S. Hamed Javadi  A. Peiravi

Electrical Engineering Department, Ferdowsi University of Mashhad, Mashhad, Iran
E-mail: hamed.javadi@gmail.com

Abstract: The authors define the probability of receiving correct decisions from all the clusters by the data fusion centre as the reliability of distributed detection in clustered wireless sensor networks and formulate it in two cases of parallel and serial distributed detection. An energy-efficient distributed detection method – called hybrid distributed detection – is also proposed in which distributed detection is performed during hop-by-hop transmission of data from the cluster nodes to the cluster head. It is shown that this method conserves much more energy than previously proposed methods and results in considerable improvement in network reliability.

1 Introduction

In a wireless sensor network (WSN), a large number of wireless devices are deployed in an environment in order to perform tasks such as measurements, event detection and target tracking. The sensor nodes send their information to a data fusion centre (FC) in an ad hoc manner, that is, each node acts as a router to data to the FC. Since battery is usually used as the sensor node's power supply and its replacement is almost impossible in many applications, energy-efficiency is the most important challenge of WSNs.

In order to conserve energy, the sensor nodes may be switched on and off periodically with a low duty cycle. Several medium access control (MAC)-layer protocols such as IEEE 802.15.4 [1] and S-MAC [2] have been presented to be used to achieve this. In addition, several energy-efficient routing protocols have been introduced. Akkaya and Younis [3] classified routing protocols of WSNs into three basic types: data-centric, location-based and hierarchical.

In this paper, the focus is on hierarchical routing protocols in which energy conservation is carried out by clustering the nodes. Each cluster would have a cluster head (CH) in which the cluster nodes’ data is aggregated and then forwarded to an FC. In homogenous WSNs, the node that acts as the CH should be changed periodically in order to balance energy dissipation between the nodes of the cluster. Some instances of hierarchical routing protocols are LEACH [4], TEEN [5], APTEEN [6], PEGASIS [7] and several heuristic energy-efficient methods as those presented in [8, 9].

In many applications, the main task of sensor nodes is to report the occurrence of an event to an FC. Then, the FC decides about the occurrence of that event based on a specific rule.

Signal detection in a distributed manner is a problem addressed extensively in the literature [10–13]. The mentioned works consider the binary hypothesis detection problem for simplicity and try to formulate the analysis of detection performance considering some logical assumptions.

Distributed detection problem was first considered by Tenny and Sandell [11] where the optimal rule of decision fusion is obtained for the two-sensor case. It is shown that the optimal decision rules of the sensors are coupled to each other in general. However, some reasonable assumptions such as independent observation noise would result in decoupled decision rules in sensors and FC.

An Maximum A Posteriori (MAP)-based optimal decision fusion is proposed by Chair and Varshney [12] in which all sensors should periodically transmit their probabilities of detection and false alarm to the FC. This fusion rule is not practical in WSNs with very limited energy and bandwidth resources. Niu and Varshney [10] propose the counting rule as an alternative to the theoretically optimal method. In counting rule, the FC first counts the number of decisions made by sensors and then compares it with a threshold in order to make a final decision.

It has been proven in [13] that for a k-out-of-n fusion rule (counting rule) with either Neyman–Pearson or Bayesian criterion, a likelihood ratio test at each individual sensor node would be optimal for the fusion performance if the sensor decisions are conditionally independent. Considering the binary hypothesis testing, Niu and Varshney [14] derived the system level probability of detection in a random deployed sensor network analytically for both lossless wireless channels and wireless channels whose error rates are not negligible.

In a scenario called censoring sensors, proposed by Rago et al. [15] and Jiang and Chen [16], sensor nodes do not send their data under the detection of one hypothesis whose a priori probability is more than the other one. This method has been shown in [16] to be suitable in WSNs as it reduces the communication overhead dramatically and allows incoherent detection and hence cancels off the
requirement for the phase information of transmission channels.

Multi-hop data transmission is usually preferred to direct
transmission because of energy-efficiency and
environmental limitations. Yang et al. [17] suggest several
routing algorithms for optimising energy dissipation and
detection performance simultaneously. In their scheme,
each sensor node has to send its observed data to the FC
and then, the FC performs centralised detection based on
the nodes’ observations. The drawback of the proposed
algorithms is wasting resources, although it usually yields a
to-detection performance. In contrast, a multi-hop
distributed detection is presented and analysed by Tian and
Coyle in [18] in which local measurement errors and
communication errors are introduced as the sources of final
decision error probability in the FC.

In this paper, performance of distributed detection in
clustered WSNs is formulated in terms of reliability of
distributed detection and decision error probability. A novel
method of performing energy-efficient distributed detection
is also proposed. In this method, distributed detection is
performed not only in the CH but also during hop-by-hop
data transmission from cluster nodes to the CH. In fact,
each node makes its decision based on its observation and
its received decisions, and then just transmits its decision to
the next node. In other words, each cluster node acts as a
local FC, not just as a router of information to the CH as
proposed in [17, 18]. It is shown that this method gives a
reliable detection and conserves much more energy
compared with other methods.

Furthermore, an algorithm is proposed to analyse detection
performance in multi-hop clustered WSNs. The results may
be used to obtain clustering schemes in which detection
performance, energy dissipation and the mean delay are
optimised simultaneously.

The rest of this paper is organised as follows. In Section 2,
the reliability of detection is defined and analysed in the cases
of distributed serial and parallel detection and centralised
detection. Hybrid distributed detection (HDD) is introduced
and analysed in Section 3. The paper is finally concluded in
Section 4.

2 Reliability of distributed detection

In event detection applications in clustered WSNs, the cluster
nodes make decisions about the occurrence of an event and
send their data to their CH. Then, the CH decides whether
or not the event has occurred in that cluster and sends its
decision to an FC. That is, a distributed detection is
performed in each cluster. The FC detects the clusters
(regions) in which the event has occurred. As the FCs
decide based on the received data from the CHs,
receiving correct decisions from the CHs is a crucial metric.

Definition: Define the probability of receiving correct decisions
from all the clusters of the network at the FC as the reliability
of distributed detection and denote it by $R_{DD}$ given by

$$R_{DD} = \prod_{i=1}^{N_C} (1 - \text{DEP}_i)$$ (1)

where $N_C$ and $\text{DEP}_i$ denote the number of the clusters in the
network and the probability of an erroneous decision made in
the $i$th cluster, respectively.

In this study, the reliability of distributed detection in both
parallel and serial configurations is analysed. Then the results
are used in the general case of a multi-hop cluster. It is
assumed that each sensor node performs a binary detection
between hypotheses $H_0$ and $H_1$ (event occurrence) and
sends its decision just in case of detection of $H_1$, that is,
nodes do not send any data in case of detecting $H_0$.

Throughout this paper, it is assumed that sensor
observations are statistically independent of each other. In
case of dependent observations, each sensor’s optimal
decision depends on the observations of other sensors. This
case has been studied in [19–21] and is beyond the scope of
this study.

In this section, the performance of centralised detection is
analysed in Section 2.1. Then, the performance of
distributed detection is formulated using the above
definition of reliability in Sections 2.2 and 2.3.

2.1 Reliability of centralised detection

In centralised detection, all sensor nodes send their
observations to an FC. Then, the FC decides about the
occurrence of an event based on the received observations.
Assume that all sensor nodes in a network are synchronised
such that no interference occurs and communication error is
negligible. The following assumptions are made in order to
analyse the performance of centralised detection.

Assumptions:

1. Each sensor’s observation under the two hypotheses $H_0$
   and $H_1$ is as follows

$$y_i = \begin{cases} m + v_i, & H_1 \\ v_i, & H_0 \end{cases}$$ (2)

where $y_i$ is the sensor is observation contaminated with noise $v_i$
and $m$ is the supposed level of received signal under
hypothesis $H_1$.

2. Sensor observations suffer from Gaussian noise with variance $\sigma$ ($v_i \sim \mathcal{N}(0, \sigma)$) and are independent of each other.

Using the above assumptions, it is straightforward to show
that for sufficiently large number of nodes (e.g. $n > 5$) the
probabilities of detection and false alarm in centralised
detection could be estimated using (3) and (4), respectively

$$P_{D,\text{centralised}} = 0.5 \text{erfc} \left( -\frac{n \sqrt{\text{SNR}}}{\sqrt{8}} \right)^n$$ (3)

$$P_{FA,\text{centralised}} = 0.5 \text{erfc} \left( \frac{n \sqrt{\text{SNR}}}{\sqrt{8}} \right)^n$$ (4)

where $\text{erfc}(x)$ is the complementary error function as defined
in (5)

$$\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} \exp(-z^2) \, dz$$ (5)

and SNR is the signal-to-noise ratio given in (6)

$$\text{SNR} = \frac{m^2}{\sigma^2}$$ (6)

which could be also obtained simply using the definition of
signal power, that is

\[
\text{SNR} = \frac{S_m}{S_v} = \frac{1/T \int_0^T m^2 \, dt}{1/T \int_0^T v^2 \, dt}
\]

where \(S_m\) and \(S_v\) are the power of signal \(m\) and noise \(v\), respectively, and \(T\) is the duration during which a sensor observes the environment (\(m\) is assumed to be constant during \(T\)).

Thus, decision error probability (DEP) and reliability of detection in centralised detection could be obtained using

\[
\text{DEP}_{\text{centralised}} = (1 - p)P_{\text{FA,centralised}} + p(1 - P_{\text{D,centralised}}) \quad (7)
\]

\[
R_{\text{CD}} = 1 - \text{DEP}_{\text{centralised}} \quad (8)
\]

where \(p = P(H_1)\) is assumed to be the same for all nodes. Assuming \(p = 0.5\), DEP against the number of nodes \(n\) is shown in Fig. 1 for several values of SNR. It is shown that centralised detection performs very well since the FC decides about the occurrence of the event based on all measurements of the sensor nodes. However, as sensor nodes have to send their observation, it wastes resources of the network and reduces the network’s lifetime.

### 2.2 Reliability of serial distributed detection

Multi-hop transmission of data to the FC has been proposed as a solution to overcome problems such as obstacles and long distances. It also conserves much more energy than transmitting data directly to the FC [22 pp. 81–83]. In serial distributed detection, as shown in Fig. 2, each sensor’s decision, except the first one, is made based on its observation and its received decision.

**Theorem 1:** In serial distributed detection, assuming that each node’s received decision and observation are statistically independent, the probabilities of detection and false alarm in the \(n\)th node of the serial chain are given by (9) and (10), respectively

\[
P_{D_n} = P_{D_{n-1}} \int_{y_n \cdot \alpha(y_n, p) \geq (1 - P_{\text{FA}_{n-1}})/P_{\text{D}_{n-1}}} P(y_n | H_1)
\]

\[+ (1 - P_{D_{n-1}}) \int_{y_n \cdot \alpha(y_n, p) \geq (1 - P_{\text{FA}_{n-1}})/1 - P_{\text{D}_{n-1}}} P(y_n | H_0)
\] 

(9)

\[
P_{\text{FA}_n} = P_{\text{FA}_{n-1}} \int_{y_n \cdot \alpha(y_n, p) \geq (1 - P_{\text{FA}_{n-1}})/P_{\text{D}_{n-1}}} P(y_n | H_0)
\]

\[+ (1 - P_{\text{FA}_{n-1}}) \int_{y_n \cdot \alpha(y_n, p) \geq (1 - P_{\text{FA}_{n-1}})/1 - P_{\text{D}_{n-1}}} P(y_n | H_0)
\] 

(10)

where \(y_n\) is the observation of the \(n\)th node and \(\alpha(y_n, p)\) is given by

\[
\alpha(y_n, p) = \frac{P(y_n | H_1)}{P(y_n | H_0)} \frac{p}{1 - p}
\] 

(11)

in which \(p = P(H_1)\).

**Proof:** See Appendix.

Using the above theorem, DEP and the reliability of distributed detection of the \(n\)th node in the serial chain are given by (12) and (13), respectively

\[
\text{DEP}_n = p(1 - P_{D_n}) + (1 - p)P_{\text{FA}_n}
\] 

(12)

\[R_{\text{D}_n} = 1 - \text{DEP}_n
\] 

(13)

In serial binary signal detection, each sensor’s observation under the two hypotheses is given by (14)

\[
y_i = \begin{cases} m_i + v_i & H_1 \\ v_i & H_0 \end{cases}
\] 

(14)

where \(y_i\) is the observation of the sensor \(i\) contaminated with noise \(v_i\), and \(m_i\) is the level of the received signal by sensor \(i\) under hypothesis \(H_1\) (event occurrence). Assuming that the nodes suffer from white noise with variance \(\sigma^2\), SNR at sensor \(i\) can be defined as \(\text{SNR}_i = (m_i^2/\sigma^2)\).

Let SNR be the same for all nodes (\(\text{SNR}_i = \text{SNR}\)). In general, different values of SNR are measured by sensor nodes. However, the same measured SNR assumption will be exploited in order to evaluate detection performance and
obtain some useful results. Using (10), $P_{FA}$ in the $n$th node of the serial chain is (see (15))

Assuming $p = 0.5$, DEP in the $n$th node of the serial chain would be $DEP_n = P_{FA_n}$ which is given in (15) and shown in Fig. 3 as a function of the number of serial nodes for various SNR values.

### 2.2.1 Energy-efficient serial distributed detection

In serial distributed detection, each sensor node uses its received decision in order to decide with a higher confidence compared with when it decides on its own. When a node receives an event occurrence decision from its prior node, it would make its decision threshold $\gamma_n$ [see (26) in Appendix] $(P_{D_{n-1}})/P_{FA_{n-1}})$ times larger and hence increase its probability of detection $P_{D_{n}}$. On the other hand, if no data are received by the node, it would detect that its prior node has detected no event. Then, it would make its own decision threshold $(1 - P_{D_{n-1}})/(1 - P_{FA_{n-1}})$ times smaller. This form of consideration of decisions of the prior node increases the reliability of detection, but it requires each node to send its $P_{D}$ and $P_{FA}$ in addition to its decision using more energy and bandwidth.

One solution to save energy and bandwidth would be to preset a reasonable $P_{D_{n-1}}$ and $P_{FA_{n-1}}$, for example, 0.8 for $P_{D_{n-1}}$ and 0.1 for $P_{FA_{n-1}}$ in each node of a serial chain. In this way, each node would need to send just its decision; however, detection performance would not be optimal.

### 2.2.2 Delay analysis

Delay is one of the most important issues in serial distributed detection. To analyse delay performance, a serial chain of completely synchronised nodes is considered.

In delay analysis, we ignore the processing time spent in the nodes. Although data exchange in WSNs is usually performed at low-bit rates, data processing is carried out using very fast microcontrollers. Each node’s decision is transmitted via a suitable protocol in a $k$-bit frame including the source address, destination address, error check sequence, possibly along with other fields, for example, for security purposes.

$$
P_{FA_n} = 0.5P_{FA_{n-1}} \text{erfc} \left( \frac{\sqrt{\text{SNR}}}{2\sqrt{2}} + \frac{1}{\sqrt{2\text{SNR}}} \ln \left( \frac{P_{FA_{n-1}}}{P_{D_{n-1}}} \right) \right) + 0.5(1 - P_{FA_{n-1}}) \text{erfc} \left( \frac{\sqrt{\text{SNR}}}{2\sqrt{2}} + \frac{1}{\sqrt{2\text{SNR}}} \ln \left( \frac{1 - P_{FA_{n-1}}}{1 - P_{D_{n-1}}} \right) \right)$$

Let us consider three possible methods for distributed detection. In the first method, the first node of the serial chain (node 1) sends its decision data to node 2 in a $k$-bit frame (sending nothing means detection of no event, but the delay of its transmission should be included for synchronisation). Node 2 relays the first node’s decision data and then transmits its decision immediately. In a similar way, each node of the serial chain relays its received frames and then transmits its decision data. This process is continued until the frames reach the FC of the serial chain.

In the second method, serial distributed detection is performed. However, in each node, a predefined value of the probabilities of detection and false alarm of each node’s prior node is set in order to save energy and bandwidth. In the third method, each node has to send its probabilities of detection and false alarm in addition to its decision data. It is assumed that each probability is transmitted using 1 byte.

The delays in the three methods are compared in Table 1. It can be seen that the use of serial distributed detection benefits not only from low-energy consumption but also from reduced delay.

### 2.3 Reliability of parallel distributed detection

In parallel distributed detection, each node sends its decision directly to an FC and then the FC decides about event occurrence using a specific fusion rule. Here, we consider a clustered WSN in which parallel distributed detection is performed in each cluster and the CH acts as the FC.

In this configuration, transmitting data from the cluster nodes to the CH as the FC may be carried out using a suitable MAC protocol like 802.15.4 [1]. Using this protocol, the CH, acting as the Personal Area Network coordinator, transmits a data packet called superframe to the cluster nodes periodically. The node that acts as the CH and the time slot each node should use to send its decision are defined in the beacon field of the superframe. As the nodes perform the binary detection, their decision may include just one bit. Using this method and also a suitable transmitting energy level, the communication error would be very negligible, if the nodes are synchronised accurately.

Neglecting the communication error, the probability of receiving incorrect decision from the $j$th node would be

$$
P_{ej} = pP_{M_j} + (1 - p)P_{FA_j}$$

where $P_{M_j}$ and $P_{FA_j}$ denote the probabilities of miss and false

### Table 1 Delay performance of different methods of distributed detection in a fully synchronised serial chain of sensor nodes

<table>
<thead>
<tr>
<th>Method</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmitting each node’s decision hop-by-hop</td>
<td>$\frac{n(n + 1)}{2BR}$</td>
</tr>
<tr>
<td>serial distributed detection (without sending each node’s $P_D$ and $P_{FA}$)</td>
<td>$nk/BR$</td>
</tr>
<tr>
<td>serial distributed detection (with sending each node’s $P_D$ and $P_{FA}$)</td>
<td>$\frac{n(k + 2)}{BR}$</td>
</tr>
</tbody>
</table>

*BR is the bit rate
alarm in node \( j \), respectively. The nodes’ observations are assumed to be spatially and temporally i.i.d. It is also assumed that the cluster nodes suffer from i.i.d. measurement noise. Thus, the probability of receiving incorrect decision from each node would be the same, that is, \( P_{e_i} = P_{e_j} \) for each node.

For simplicity, it is also assumed that \( p = 0.5 \). Using our assumptions, it is shown in [18] that the decision error probability in cluster \( i \), \( \text{DEP}_i \), is obtained by (17)

\[
\text{DEP}_i = \sum_{j=0}^{n_i-1} \left( \frac{n_i}{j} \right) p_j^j(1-p_j)^{n_i-j}
\]

where \( n_i \) is the number of nodes in the cluster \( i \) ignoring its CH and \( (n_i/2) \) denotes the largest integer value equal to or less than \( (n_i/2) \). For the general case in which \( p \neq 0.5 \), the summation would not start from \( (n_i/2) \) (refer to Tian and Coyle [18]).

Thus, the reliability of distributed detection in a network including \( N_C \) clusters could be obtained using (18).

\[
R_{DD} = \prod_{i=1}^{N_C} \left( 1 - \sum_{j=0}^{n_i-1} \left( \frac{n_i}{j} \right) p_j^j(1-p_j)^{n_i-j} \right)
\]

Example 1: Analysing the reliability of distributed detection in a 100-node network under the presence of white noise.

If the same SNR value is measured by the sensors, the probabilities of detection and miss in each sensor are obtained simply using

\[
P_{FA} = P_M = 0.5erfc\left(\frac{\text{SNR}}{\sqrt{8}}\right)
\]

Using (16) and assuming \( p = 0.5 \), we would have \( p_e = P_{FA} = P_M \).

DEP as a function of the number of cluster nodes and SNR is shown in Fig. 4. It could be seen that the DEP value decreases exponentially as the number of parallel nodes is increased. In addition, the DEP value for even number of nodes is less than that for odd number of nodes. The comparison between Figs. 3 and 4 shows that for a given number of nodes, the DEP in parallel distributed detection is more than the one in serial distributed detection because each sensor node in serial distributed detection obtains help from its prior nodes as mentioned in the previous subsection. Thus, decision making is performed with a higher reliability as it moves forward to the CH in the serial chain. However, in parallel distributed detection, the FC makes decision based on the decisions of the sensor nodes whose reliabilities are equal to the reliability of the first node of the serial chain.

The reliability of parallel distributed detection in (18) depends on just the number of network clusters and the number of nodes in each cluster. To analyse the effect of clustering on \( R_{DD} \) we divide a 100-node network into \( N_C \) clusters of as equally sized as possible. For example, if \( N_C = 2 \), the mean number of nodes in each cluster would be 50 and one node acts as the CH in each cluster; so, \( n_1 = n_2 = 49 \). The reliability is plotted in Fig. 5 against the number of clusters \( N_C \). It is shown that the curve is descending in general. The reason is that when the number of clusters increases, the number of nodes per cluster performing parallel distributed detection decreases causing an increase of DEP (Fig. 4). The fluctuations in the curve are because of the fluctuations between even and odd number of nodes in Fig. 4.

### 3 Hybrid distributed detection

In this section, a novel method of distributed detection is first presented noting the advantages of serial and parallel distributed detection. The method is called hybrid distributed detection since it combines serial and parallel detection in a general network configuration. Then, the analysis of its performance is presented and finally the proposed method is compared to the existing methods in term of network reliability that reflects lifetime as a function of energy.

#### 3.1 Algorithm

In a clustered WSN, transmitting data from the cluster nodes to the CH is generally carried out in a multi-hop manner because of environmental limitations and energy-efficiency. In distributed detection applications of WSNs, the distributed detection process may be performed during
transmission of the cluster nodes’ information to the CH. In fact, each cluster node could act as a local FC, that is, it makes its decision based on its observation and its received decisions from its previous nodes.

As mentioned in Section 2.2.1, the best way to save energy is by presetting suitable values for probabilities of detection and false alarm of previous node(s). Thus, the decision rule for node \(i\) in a network using the local ratio test (LRT) would be simply

\[
y_i \geq \sigma \left( 0.5 \sqrt{S_i} + \frac{1}{\sqrt{S_i}} \ln \left[ \frac{F}{D} \left( \frac{1 - F}{1 - D} \right)^{n-k} \right] \right)
\]

where \(S_i\) is the measured SNR by sensor \(i\), \(F\) and \(D\) are the preset values for the probabilities of false alarm and detection of previous nodes of node \(i\), \(k\) is the number of nodes that detect event occurrence and transmit data to node \(i\), \(n\) is the number of prior nodes of node \(i\) and \(\sigma\) is the noise standard deviation and \(c = ((1-p)/p)\) with \(p = P(H_1)\).

Using this decision rule, the threshold would be adaptive relative to its received decisions and the measured SNR. If a node’s measured SNR is high, the threshold would weigh its received decisions less and vice versa.

Note that HDD attempts to maximise detection performance and minimise false alarm rate. Less transmitted information in addition to tuning decision during hop-by-hop transmission, as shown before, would increase network performance and lifetime.

### 3.2 Performance analysis

The reliability of HDD could be obtained using Algorithm 1 (Fig. 6) in cases in which \(m\) is known. However, performance analysis of HDD is generally intractable since each node’s decision rule depends on its measured SNR. Nevertheless, the performance of HDD in a WSN could be predicted using Monte-Carlo simulations.

In Fig. 6, it is assumed that the cluster’s network graph and the nodes’ geographic information are known. If the nodes’ geographic information is not defined, it can be obtained using any of the various localisation techniques already proposed in the literature (e.g. see [23, 24]). After computing the DEP values in all the clusters of the network, the reliability of the network could be obtained using (1).

### 3.3 Performance evaluation

We are going to compute the reliability of the cluster shown in Fig. 7. In this configuration, the nodes 1, 2, 3 and 4 make their local decisions based on just their observations. The nodes 5–8 perform a serial distributed detection and the nodes 9 and the CH perform a parallel distributed detection.

In this example, it is assumed that the observations of the nodes are spatially and temporally independent and identically distributed (i.i.d.) and the cluster nodes also suffer from white measurement noise with unit variance. It is also assumed that the measured SNR in sensors are the same. Such case may occur in applications such as high-humidity detection in agriculture or high-temperature detection in fire detection. \(F = 0.2\) and \(D = 0.8\) are considered in the simulation.

![Fig. 6 Computation of reliability of HDD](image)

![Fig. 7 Multi-hop cluster used in performance evaluation](image)
The first-order radio model presented in [5] is adopted for estimations of the dissipated energy of different distributed detection methods. In this model, the dissipated energy for transmitting and receiving \( k \) bits of information in a node is given, respectively, by (20) and (21)

\[
E_{\text{trans}} = k(E_{\text{elec}} + e_{\text{amp}} \times d_j^2) \tag{20}
\]

\[
E_{\text{rec}} = k E_{\text{elec}} \tag{21}
\]

where \( E_{\text{trans}} \) is the consumed energy during transmitting \( k \) bits of information from the source node \( i \) to the destination node \( j \), \( E_{\text{elec}} \) is the energy consumed in the electronic circuitry of the sensor node, \( e_{\text{amp}} \) is the energy consumed by the transmitter amplifier for transmitting one bit of information over 1 m, \( d_j \) is the distance between the source node \( i \) and the destination node \( j \) and \( E_{\text{rec}} \) is the energy consumed during receiving \( k \) bits of information. We use the parameters \( E_{\text{elec}} = 50 \) nJ/bit and \( e_{\text{amp}} = 100 \) pJ/bit/m\(^2\) as used in [5].

To obtain a suitable metric to compare the efficiency of distributed detection methods, we define the reliability of network as follows

\[
R_N = R_{\text{DD}} P(T_{\text{network}} \geq t) \tag{22}
\]

where \( T_{\text{network}} \) is the network lifetime. One common definition of network lifetime which is adopted here is the time span from deployment to the instant the first sensor dies (e.g. because of the battery exhaustion) [25]. Based on this definition, the network lifetime would be equal with the lifetime of the sensor in which the most amount of energy is consumed. Thus, we have

\[
P(T_{\text{network}} \leq t) = P(T_{\text{sensor}} \leq t) \tag{23}
\]

where \( T_{\text{sensor}} \) is the average sensor lifetime.

Using an example, it was shown that the proposed distributed detection method is much more energy-efficient than the previously presented methods such as one-hop clusters and multi-hop clusters suggested by Tian and Coyle [18], whereas its reliability of distributed detection is still acceptable. The formulations presented in this paper may be used as a cost function together with mean delay in any of several heuristic multi-objective optimisation methods – for example, multi-objective genetic algorithms [26] and ant colony [27] – in order to obtain an optimum clustering scheme in the network, that is, arranging nodes in clusters in such a way that the network reliability and delay are simultaneously optimised.

4 Conclusions

We defined the probability of receiving correct decisions from all the cluster heads by the FC as the reliability of distributed detection in clustered multi-hop WSNs. This definition of reliability was formulated and used for the analysis of serial and parallel distributed detections in this paper. Moreover, a new distributed detection method was proposed in which each node could act as a local FC in a multi-hop clustered network, that is, distributed detection is performed during transmitting data from the cluster nodes to the cluster head.

At the end, it worth noting that although a network could reach a high degree of network reliability using hybrid detection, it would suffer from delay. This delay would be caused because of the performing serial detection in some nodes. It would also suffer from some performance degradation in case a link is broken at an intermediate stage.

5 References

1 LAN/MAN Standards Committee of the IEEE Computer Society. ‘IEEE standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – Part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (LR-WPANs)’, October 2003
Appendix: Proof of Theorem 1

Assume that the observations of the nodes are spatially and temporally i.i.d. and also the cluster nodes suffer from i.i.d. measurement noise. In this case, using MAP criterion, the decision rule in the $n$th node of the serial chain is

$$u_n = \begin{cases} 
1 & \gamma_n \geq 1 \\
0 & \text{otherwise} 
\end{cases} \quad (25)$$

where $\gamma_n$ is a decision threshold which is an MAP-based expression given by (26)

$$\gamma_n = \frac{P(H_1|y_n, r_n)}{P(H_0|y_n, r_n)} = \frac{P(y_n, r_n|H_1)P(H_1)}{P(y_n, r_n|H_0)P(H_0)} \quad (26)$$

in which $y_n$ and $r_n$ are the nth node’s observation and received decision, respectively. Actually, an LRT [10] occurs at each node in which the threshold of decision making is equal to $P(H_0)/P(H_1)$. Neglecting the communication error, $r_n = u_{n-1}$. Also, based on our assumption, $y_n$ and $r_n$ are the independent random variables. Thus

$$\gamma_n = \frac{P(u_{n-1}|H_1)}{P(u_{n-1}|H_0)} \alpha(y_n, p) \quad (27)$$

Assuming independence of the node’s observation and its received decision, the detection probability of $n$th node is computed by (28)

$$P_{D_n} = \int_{\gamma_n \geq \gamma_1} P(y_n, u_{n-1}|H_1) = \int_{\gamma_n \geq \gamma_1} P(u_{n-1}|H_1)P(y_n|H_1)$$

$$= P(u_{n-1} = 1|H_1) \int_{\gamma_n \geq \gamma_1} P(y_n|H_1) + P(u_{n-1} = 0|H_1)$$

$$\times \int_{\gamma_n \geq \gamma_1} P(y_n|H_1) \quad (28)$$

However $P_{D_{n-1}} = P(u_{n-1} = 1|H_1)$ and $1 - P_{D_{n-1}} = P(u_{n-1} = 0|H_1)$. Replacing these equations in (28), the detection probability of nth node in the serial chain is obtained using (9). Equation (10) is also obtained in a similar way.