


RESEARCH

Open Access



A comprehensive wireless sensor network reliability metric for critical Internet of Things applications

Dina Deif  and Yasser Gadallah*

Abstract

Evaluating the reliability of a wireless sensor network (WSN) deployment is a highly important task especially when the WSN is used for a critical Internet of Things (IoT) application. In this paper, we introduce a novel comprehensive reliability metric to evaluate the reliability of WSN deployments over their intended mission time. Unlike the existing studies on the topic, the proposed metric takes into account that sensor nodes (SNs) are multi-component systems that are subject to different component failures, namely, sensor, transceiver, processor, and battery failures. Consequently, SNs are modeled as three-mode (*on*, *relay*, and *off*) systems instead of the simplistic two-mode (*on* and *off*) model adopted in the existing studies. To calculate the proposed reliability metric in a computationally efficient manner, we develop a search algorithm which generates the complete path set of the given WSN deployment. Extensive experimental results demonstrate the use of the proposed metric in evaluating the reliability of several WSN deployments under different operating conditions. Results also demonstrate the computational efficiency of the developed search algorithm used for calculating the proposed metric and the significant effect of using the proposed three-mode SN model on the accuracy of the evaluated reliability.

Keywords: Wireless sensor networks, Reliability, Fault tolerance, Internet of Things, Probability of failure, Combinatorics

1 Introduction

In recent years, wireless sensor networks (WSNs) have become a versatile technology for serving a multitude of applications that include residential, industrial, commercial, healthcare, and military applications. As such, WSNs are considered one of the enabling technologies for realizing the Internet of Things (IoT) concept where they play the pivotal role of detecting events and measuring physical and environmental phenomena of interest [1]. Many of the important IoT applications served by WSNs are characterized by being mission-critical, meaning that the failure of the WSN to detect the occurrence of an event or a phenomenon in the targeted region of interest (RoI) will have serious implications [2]. Hence, it is imperative that the WSN functions properly throughout its intended mission time. This poses stringent reliability requirements on the WSN

that must be addressed in the design and deployment phase of the network.

The first step in designing a reliable WSN is to be able to evaluate the reliability of a given WSN deployment. The reliability of any multi-component system is formally defined as the “probability that a system will perform satisfactorily during its mission time when used under the stated conditions” [3]. The method by which the reliability of a specific system is evaluated varies according to the type(s) of components the system is composed of, the configuration of the system in terms of how these components are connected to each other, and the state(s) at which the system is defined to have failed. Ultimately, the reliability of the system is a function of the reliability measures of its components and evaluating the reliability of the system as a whole is a probability modeling problem.

In that context, a WSN can be viewed as a multi-component system in which the components are the sensor nodes (SNs) and the sink node(s). The mission time for a WSN can either be its intended lifetime or

* Correspondence: ygadallah@iee.org

Electronics and Communications Department, School of Sciences and Engineering, The American University in Cairo, AUC Avenue, New Cairo 11835, Egypt

the maximum time interval between scheduled maintenance operations. Hence, the WSN mission time is application-dependent and can vary greatly, ranging from a few days to a few years. If the WSN is composed of different types of SNs with different coverage profiles and capabilities, the WSN is said to be *heterogeneous*. The configuration of the WSN is determined by the way the SNs are deployed in the targeted RoI and the resulting wireless connectivity among them.

In order to identify the states at which a given WSN deployment fails, the functionality of a WSN must first be defined. The functionality of a WSN can be divided into two major elements. The first element is the sensing functionality, which is the ability of a WSN to detect all the targets or phenomena that occur inside the boundaries of the RoI during its mission time. Hence, for a WSN to be functional in terms of sensing, it must provide full coverage for the RoI area (in case of area coverage) or all the targeted locations in the RoI (in case of point coverage) during its mission time. The second element of the WSN functionality is the connectivity functionality, which is the ability of the WSN to deliver sensed data from its sources (i.e., SNs) to the designated destination (i.e., sink node(s)) during its mission time. Hence, for a WSN to be functional in terms of connectivity, any target or a phenomenon detected by one or more SNs has to be recognized at the sink node(s) through multi-hop wireless communication throughout the WSN mission time. Based on this definition of WSN functionality, a WSN is said to have failed if either of its sensing or connectivity functionality elements fail [4].

There are several issues that can affect the reliability of a WSN by compromising its functionality in terms of coverage and/or connectivity. These issues can generally be classified into SN-related and non-SN-related issues. SN-related issues are factors pertinent to the functionality of the deployed SNs, mainly, SN power failure, hardware failures, and software failures. The effect of these issues on the functionality of the network during its mission time (i.e., on the reliability of the network) can be predicted [5] as will be discussed later. These issues can be summarized as follows:

- SN power failure: the majority of the industrial and commercial SNs currently available in the market are battery-powered. Current advances in the fabrication of batteries have recently introduced highly durable batteries for SNs that can last for years (e.g., lithium thionyl chloride batteries (<http://www.tadiranbatteries.de/eng/products/lithium-thionyl-chloride-batteries/overview.asp>)) under certain conditions. Although these batteries can sustain the operation of the SNs for long periods of time, premature battery failures can still occur in practice. This can

be attributed to a myriad of reasons such as the deployment of the SNs in harsh environmental conditions (e.g., extreme temperatures or rain), incorrect handling or random failure caused by defective hardware (https://www.omnisense.com/oms_cds/media/008-002-002%20OmniSense%20FMS%20Sensor%20Battery%20Life.pdf).

- SN hardware failures: SNs are subject to random hardware failures. This is attributed to two main reasons. The first one is that most commercial SNs are cost-sensitive, meaning that they are not always built of the highest quality components. The second reason is that SNs are often subjected to harsh environmental conditions which can affect the normal operation of its components [6].
- SN software failures: SNs are prone to random permanent software failures which can render them inactive, i.e., unable to sense or communicate.

On the other hand, non-SN-related issues are factors that are external to the deployed SNs such as wireless link failures (due to fading and external interference) and excessive packet collisions (i.e., internal interference in WSNs adopting contention-based medium access control). The effect of these issues on the overall network reliability is in general difficult to predict. The authors in [7] present a thorough study on the effects of non-SN-related factors on the quality of wireless links in a WSN and show the complex and highly transient nature of these effects. Furthermore, the effects of the non-SN related issues on the WSN reliability are usually mitigated using measures such as acknowledgements and retransmissions [8].

In this paper, we derive a comprehensive WSN reliability metric, which considers the different *SN-related* reliability issues, using a combinatorial approach. We adopt the general assumptions that the WSN is heterogeneous and has an arbitrary deployment configuration (e.g., clustered or flat configuration). The functionality of the WSN is defined in terms of both network coverage and connectivity of the SNs to the sink node(s). We assume that the SNs are subject to four types of failures during the WSN mission time, namely, sensor failure, transceiver failure, processor failure, and power failure. Consequently, SNs are modeled as systems which have three modes of operation, namely, *on*, *relay*, and *off*. To calculate the proposed reliability metric in a computationally efficient manner, we develop a search algorithm which generates the complete paths set of the given WSN deployment.

The rest of this paper is organized as follows. In Section 2, we summarize the existing work on WSN reliability and highlight the contribution of this paper. In Section 3, we briefly discuss some of the fundamental

reliability concepts which we will be using throughout this paper. The assumptions and derivation of the proposed reliability metric are presented in Section 4. In Section 5, we present the developed search algorithm which is used to evaluate the reliability of WSN deployments based on the proposed metric. Section 6 presents the experimental results obtained from applying the proposed metric to case study surveillance WSN deployments. Finally, the paper is concluded in Section 7.

2 Related work on wireless sensor network reliability

Several studies have addressed the issue of evaluating or estimating the reliability of WSNs. In this section, we review the most significant of these studies and discuss their scope and limitations. Based on this discussion, we highlight the scope and contribution of the reliability metric proposed in this paper. We classify the existing studies on WSN reliability into two major tracks. The first track focuses on evaluating the reliability of a specific aspect of WSN functionality (such as packet transmission reliability) and/or to evaluate the reliability for one or more *parts* of the WSN (such as a single cluster in a cluster-based deployment). The studies which belong to the first track may or may not assume that SNs are subject to random failures and battery energy depletion. On the other hand, the second track focuses on evaluating the reliability of a WSN as a whole, either as a function of time or as a probability over a given network mission time, assuming that SNs are subject to random failures. Studies which belong to the second track define WSN functionality in terms of coverage and/or connectivity and assume that SNs are modeled as a two-mode device (either *on* or *off*) and have a given probability of failure during the mission time of the network.

We begin by reviewing studies which belong to the first track. The studies in [9] and [10] address the problem of evaluating the reliability of SN clusters in WSNs characterized by cluster-based deployments subject to random SN failures. In both studies, the authors assume that the SN clusters are non-overlapping and that each cluster has a designated cluster head which acts as a relay between the SNs in the cluster and the sink node. In [9], the authors define the reliability of a cluster as the probability of successful message delivery between the sink node and the cluster head. The authors in [10] define the reliability of the WSN as the probability that the geographical area of each cluster in the WSN is fully covered by its SNs and that the cluster head has at least one functional direct or multi-hop wireless path to the sink node. Based on this definition, they derive an expression for the reliability of each individual cluster and use a Monte Carlo (MC) simulation approach to

estimate it. The main limitation of the studies in [9] and [10] is that the reliability of the WSN as a whole in terms of the reliability of its constituent clusters is not evaluated. In addition, the proposed definitions of reliability cannot be extended to WSNs with different deployment configurations such as flat deployments which are non-hierarchical.

In [11], the authors propose a model for evaluating the reliability of disjoint areas in a WSN subject to two types of failure events, namely, SN failures due to battery depletion and link failures. Their proposed approach depends on dividing the targeted RoI into disjoint areas or target regions. For each region, a reliability model is constructed using a reliability block diagram (RBD) [3], which depends on the number of SNs monitoring the target region, their relative location from the sink node, and the routing protocol used in the network. There are two drawbacks of the proposed reliability modeling proposed in [11]. The first drawback is that the model does not provide a method by which the reliability of the entire WSN deployment can be evaluated in terms of the reliability of its regions. The second drawback is that the reliability modeling is carried out under the assumption that the probabilities of link failures are known and are constant throughout the lifetime of the WSN. This assumption is unrealistic since link quality is affected by numerous factors such as multi-path effects, shadowing (due to static and mobile obstacles), and interference. The effect of these factors on link quality varies significantly and rapidly in time and space [7] and hence, unlike SN-related factors, cannot be reduced to a constant probability of failure throughout WSN mission time. In [12], the authors consider the problem of evaluating the transmission reliability of cluster-based and mesh-based WSN deployments. They define transmission reliability as the ratio of the packets received by a destination node to the whole packets generated by the transmission for a given period of time. They present transmission reliability evaluation models for the uplink and downlink traffic based on the assumptions that SNs are not subject to any hardware failures and that SNs only fail when their initial battery energy is exhausted. Although the time-dependent models presented in [12] can help assess the transmission reliability over time for a given routing strategy, they are limited by the assumption that SNs cannot fail due to random hardware failures unrelated to battery exhaustion. Also, it is not possible to use the study in [12] to calculate or estimate the reliability of the WSN over a given mission time since coverage functionality is not considered.

The study in [13] considers the problem of evaluating the reliability of the sink node decisions in WSNs targeted for intrusion detection applications. The authors model the detection mechanism of the sink node of an

intrusion, based on the aggregated data from several SNs in the network, as a weighted voting system (WVS). They assume that both the SNs and the wireless links between the SNs and the sink node have known mis-detection probabilities. Based on these assumptions, they derive the reliability of the sink's WVS using the universal generating function (UGF) method. Similar to the study in [12], the scope of the study in [13] does not include evaluating the reliability of the WSN as a whole over a given mission time, since it is restricted to evaluating the reliability of detecting a single target/phenomena based on a fraction of the SNs in the WSN.

On the other hand, the studies in [14, 15] belong to the second track since they address the reliability of SN systems or WSNs as a whole of non-hierarchical deployment configurations subject to random SN failures. In [14], the authors address the problem of evaluating the reliability of WSNs designed for industrial inventory management. They assume that for the purposes of this specific application, the data collected by each SN are stored redundantly on several other SNs to account for random SN failures. Accordingly, the WSN is deemed functional as long as there is a sufficient number of functional SNs that are both connected to each other and to the sink node. Based on this definition of network functionality and the assumption that the WSN deployment is homogeneous, the reliability evaluation problem is reduced to the famous K -out-of- N reliability problem (<http://www.reliabilityanalytics.com/blog/2011/09/02/reliability-modeling-k-out-of-n-configuration/>). The authors also present a Monte Carlo (MC) simulation approach similar to that proposed in [10] to estimate the reliability of the WSN at hand. However, the reliability evaluation and estimation approaches proposed in [14] are based on a very restrictive definition of network functionality. Consequently, they cannot be applied to other WSN applications (e.g., surveillance and monitoring applications) where the functionality of the network is dependent not only on the number of SNs connected to the sink node but also on the network coverage. Also, the proposed approaches do not support network heterogeneity which is a major limitation since real-world deployments are often heterogeneous.

The authors in [16] propose a reliability metric for SN systems designed for surveillance purposes subject to random SN failures. They assume an arbitrary deployment configuration where SNs can monitor multiple target locations in the RoI and that each target location can be monitored by multiple SNs. They also assume that the surveillance SN system can be heterogeneous. The reliability of the system is defined as the probability that all target locations are monitored by at least one SN. The authors use a combinatorial approach to formulate the proposed reliability metric and present a search

algorithm to calculate the proposed reliability metric in a time-efficient manner. The main limitation of the proposed metric is that system functionality is assumed to be in terms of the degree of target locations coverage only. Connectivity between SNs to form a wireless network is not considered.

The study in [17] propose a method for evaluating the reliability of WSNs designed for industrial IoT applications based on the automatic generation of fault trees (FTs). The proposed method requires the network failure conditions as inputs to enable the generation of the corresponding network FT and compute the network reliability. A network failure condition is defined as a combination of SNs which if fail will lead to the failure of the WSN in terms of network coverage only and not connectivity to the sink. To address the connectivity part of the network functionality, the authors propose a depth-first search algorithm that finds all the paths between SNs belonging to the network failure conditions and the sink node. The study in [17] is extended in [15] by assuming that the WSN is also subject to permanent wireless link failures in addition to SN failures under the same assumptions adopted in [17]. In both studies, the authors in [17] and [15] did not address the computational efficiency of their approach.

In this study, we focus on the second track, i.e., on the problem of evaluating the reliability of the WSN a whole, defined as the probability that the WSN is functional during a given mission time, assuming that SNs are subject to random permanent failures. Based on the above discussion, existing studies in that track all assume that SNs have only two modes of operation, either *on* or *off*. If an SN is *on*, it is assumed to be functional in terms of both sensing its surrounding environment and communicating wirelessly with its neighbors. If it is *off*, then the SN has failed permanently due to one or more of the SN-related reliability issues outlined in Section 1. This representation is not accurate since most commercial SNs are composed of multiple independent chips that carry out different functions, with each having its own probability of failure during the network's mission time.

A more accurate model considers the SN as a multi-component system [18]. Based on this model, an SN has three modes of operation. These modes of operation are *on*, *relay*, and *off*. The definitions of the *on* and *off* modes are the same as discussed above, while the *relay* mode occurs when the SN is unable to perform its sensory function but it is still able to communicate wirelessly with its neighbors. This mode of operation occurs when the SN's sensor(s) hardware fails while its transceiver, processor, and battery are in working condition. Adopting this SN model has two main advantages. The first one is that it provides a more accurate evaluation of WSN reliability, assuming that the network functionality

is adequately defined in terms of both network coverage and connectivity. The addition of the *relay* mode to the SN model provides a more accurate evaluation of WSN reliability because it avoids the *under-evaluation* of the WSN reliability when the conventional two-mode SN model is used. Under-evaluation of the reliability of the network becomes an issue when the reliability is used as a requirement/constraint for WSN deployment. In that case, the network designer aims to deploy sufficient SNs to achieve a minimum level of network reliability while minimizing the number of deployed SNs, i.e., minimizing the deployment cost. In that case, under-evaluating the reliability of a given deployment can lead to an unnecessary increase in the deployment cost. The second advantage is that it enables the network designer to isolate the effect of the quality (i.e., reliability) of the individual components of the deployed SNs (i.e., sensor, transceiver, processor and power unit) on the overall reliability of the WSN. This is discussed in more details in Section 4.1.

In this paper, we derive a comprehensive WSN reliability metric which takes into account the different SN-related reliability issues using a combinatorial approach. Compared to the existing reliability evaluation and estimation approaches, the strengths of our proposed metric can be summarized in the following points:

- Network functionality is defined in terms of both network coverage of a predefined set of target locations in the RoI and connectivity to the designated sink node.
- No specific network deployment configuration is assumed in the proposed model. We assume an arbitrary deployment configuration where each deployed SN may monitor multiple target locations in the RoI and each target location may be monitored by multiple SNs. All SNs can communicate wirelessly with their neighbors, i.e., no imposed communication hierarchy.
- The WSN can be heterogeneous; it can consist of more than one type of SNs, each characterized by a different coverage profile and set of capabilities.
- A more realistic SN model is adopted in the derivation of the proposed metric where an SN has three modes of operation instead of the two-mode model used in the existing studies.
- Each SN type is characterized by four different probabilities of failure during the mission time of the network (namely, sensor, transceiver, processor, and battery probabilities of failure) instead of a single SN probability of failure, as it is the case in the existing studies.
- A search algorithm is developed to calculate the propose reliability metric in a computationally efficient manner.

In this study, we assume that wireless links between SNs are not subject failure. This assumption is justified as follows. Wireless link quality is affected by numerous factors such as multi-path effects, shadowing (due to static and mobile obstacles), and interference. The effect of these factors on link quality varies significantly and rapidly in time and space [7] and hence, unlike SN-related factors, cannot be reduced to a constant probability of failure throughout WSN mission time. On the other hand, permanent wireless link failures are mainly due to a complete failure (i.e., a failure in the transceiver, processor, or battery) in one or both SNs at the ends of the link [19]. In the proposed metric in this paper, this type of failure is taken into consideration since we assume that each of the main SN components are subject to failure with a given probability of failure during the WSN mission time.

3 Fundamental reliability concepts

In this section, we discuss some of the fundamental definitions and concepts related to the evaluation of multi-component systems' reliability which we will be using throughout this paper.

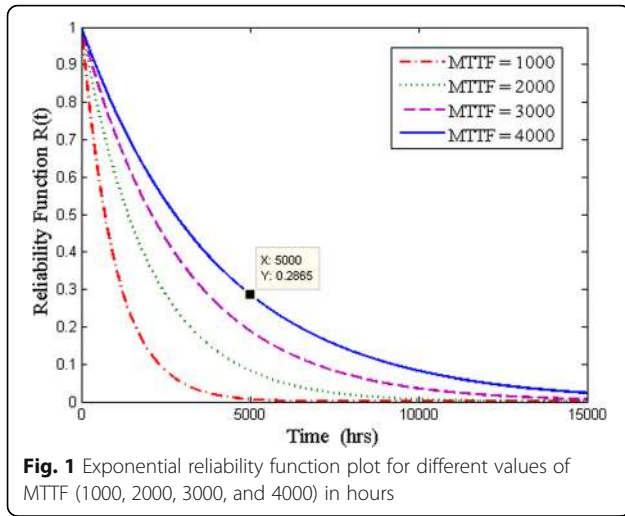
3.1 Component reliability function and component reliability

The main objective of reliability modeling is to express the reliability of a given system in terms of the reliability measures of its constituent components. There are two main reliability measures for any device or component. The first measure is the reliability function $R_c(t)$, which is used to estimate the probability that the device or component will continue to function beyond a time duration of length t [3]. The second reliability measure is based on the fact that for most practical purposes, a device or component is only required to function during the specified mission time T_m of the system it belongs to. In this case, the reliability function $R_c(t)$ can be substituted by the reliability of the device. The reliability of a device, R_c , is simply defined as the probability that the device will continue to function throughout the mission time of the system. Accordingly, the probability of failure of the device during T_m is equal to $1 - R_c(T_m) = 1 - R_c$ [3].

For example, Fig. 1 shows an exponential reliability function, which is one of the simplest functions used in modeling the reliability of electronic components. The exponential reliability function which is $R_c(t)$ is given by the following equation:

$$R_c(t) = e^{-\alpha t}, \quad (1)$$

where α is the estimated failure rate of the component per unit of measurement (e.g., hour, year, cycle) and is



equal to the reciprocal of its mean time to fail (MTTF). From the reliability curves in Fig. 1, we can estimate the reliability at $t = 5000$ h for $\alpha = 1/4000$ (i.e., for $MTTF = 4000$) to be 0.287. This in turn means that there is a $1 - 0.287 = 0.713$ chance that the component will fail during this time interval, i.e., the probability of failure during this time interval is 0.713.

Although the exponential reliability function is commonly used in reliability engineering due to its simplicity, it usually leads to inaccurate estimations of the probabilities of failures. This is because this type of function is based on the assumption that the component has a constant failure rate, which means that its performance does not degrade with time. To obtain a more accurate model for the reliability function of a given electronic device, reliability engineers carry out rigorous reliability testing techniques and/or gather empirical data on the device in service [3]. For example, qualitative and quantitative accelerated reliability testing is used to identify probable hardware failures of SNs and estimate the probability of their occurrence [5].

3.2 Combinatorial approach to system reliability evaluation

Combinatorics is a proven useful tool in evaluating and estimating the reliability of complex systems and networks [20, 21]. The fundamental premise of the combinatorial approach to reliability evaluation is that the reliability of any system can be computed by means of evaluating the system's structure function for every possible state of the system. To explain this concept, consider a system S which consists of n components, i.e., $S = \{1, 2, \dots, n\}$. Each component can only have two distinct states: it can either be functional or *on* or it can fail or be *off*. Let the binary variable π_i be the state indicator of component i as follows:

$$\pi_i = \begin{cases} 1, & \text{if component } i \text{ is on} \\ 0, & \text{if component } i \text{ is off} \end{cases} \quad (2)$$

A state π of the system S is a description of the states of all its components, hence $\pi = \{\pi_i\}$ for $i = 1, \dots, n$. Let Π be the set of all possible states of S . The structure function of S , denoted $f(\pi)$, is a binary function that indicates whether the system is working under a given state according to the following equation:

$$f(\pi) = \begin{cases} 1, & S \text{ is functional} \\ 0, & S \text{ has failed} \end{cases} \quad (3)$$

Based on the above definitions, the reliability of S , denoted by $R(S)$, can be calculated using the following equation:

$$R(S) = \text{Prob}(f(\pi) = 1) = \sum_{\pi \in \Pi} f(\pi) \cdot \text{Prob}(\pi) \quad (4)$$

To calculate $R(S)$ using (4), the conditions necessary for S to be functional must be defined and the probability of any system state must be evaluated in terms of the reliabilities (or probabilities of failure) of the system's components, assuming that the system has a specified mission time T_m . Theoretically, $f(\pi)$ must be evaluated for all the possible system states $\pi \in \Pi$ to calculate $R(S)$ using this approach. However, following this extensive method in reliability calculation poses a computational problem for systems of a practical scale. For example, a system composed of 30 components which fail independently has 2^{30} states. Therefore, a tremendous amount of time is required to calculate $R(S)$ which grows exponentially with the number of components in the system. This computational problem is mitigated by the use of more efficient methods (e.g., reliability block diagram (RBD), fault tree (FT), and search algorithms) that attempt to find all the system's path sets or cut sets [20].

To define a system's path and cut, let $S_1(\pi)$ be the set of functioning components, i.e., components in the *on* state, in S for a given system state π and $S_0(\pi)$ be the set of failed components, i.e., components in the *off* state. $S_1(\pi)$ and $S_0(\pi)$ can be expressed by the following equations:

$$S_1(\pi) \equiv \{i \mid \pi_i = 1, i \in S\}, \quad (5)$$

$$S_0(\pi) \equiv \{i \mid \pi_i = 0, i \in S\}, \quad (6)$$

where $S_1(\pi) \cup S_0(\pi) = S$. A state π of the system S is called a path if $f(\pi) = 1$. In that case, the corresponding path set is the set $S_1(\pi)$, i.e., a path set is the set of components whose simultaneous functional state guarantees that the overall system is functional. On the other hand, a state π of the system S is called a cut if $f(\pi) = 0$. In this case, the corresponding cut set is the set $S_0(\pi)$. That

is, a cut set is the set of components whose simultaneous failure results in the failure of the overall system. If all the path sets or alternatively all the cut sets of a system \mathcal{S} are known, we can rewrite (4) as follows:

$$R(\mathcal{S}) = \sum_{\pi \in \Pi_1} \text{Prob}(\pi) = 1 - \sum_{\pi \in \Pi_0} \text{Prob}(\pi), \quad (7)$$

where Π_1 is the set of all the paths of \mathcal{S} (i.e., the complete paths set of \mathcal{S}) and Π_0 is the corresponding set containing all the cuts of \mathcal{S} (i.e., the complete cuts set of \mathcal{S}) such that $\Pi_1 \cup \Pi_0 = \Pi$. For example, a simple system of n components connected in series has only one path set which is equal to the system set $\mathcal{S} = \{1, 2, \dots, n\}$ and has $\sum_{k=1}^n C_k^n$ cut sets. Therefore, it is simpler to express its reliability as $R(\mathcal{S}_{\text{series}}) = \text{Prob}(\pi = \{\pi_i = 1, \forall i = 1, \dots, n\}) = \prod_{i=1}^n R_i$, where R_i is the reliability of the i^{th} component during the system's mission time. On the other hand, a system of n components connected in parallel has only one cut set which is equal to \mathcal{S} and has $\sum_{k=1}^n C_k^n$ path sets. Hence, the system's reliability can be expressed as $R(\mathcal{S}_{\text{parallel}}) = 1 - \text{Prob}(\pi = \{\pi_i = 0, \forall i = 1, \dots, n\}) = 1 - \prod_{i=1}^n (1 - R_i)$.

4 Reliability of wireless sensor networks

In this section, we use the combinatorial approach outlined in Section 3 to derive the reliability of a WSN with an arbitrary deployment configuration. We start by modeling the SN as a multi-component system and identifying its different states and modes of operation. Then, we present the WSN model and define the conditions required for the WSN to be deemed in working condition. Finally, we derive the reliability of the WSN in terms of its structure function and the probabilities of failure of its constituent SNs' hardware components.

4.1 Sensor node model

Although SNs vary greatly in terms of their capabilities (e.g., processing power, battery capacity), there are four fundamental chips or components that are common in all SNs [22]: a sensing unit(s) or simply sensor(s), a radio unit or transceiver, a processing and memory unit or processor, and a power unit or battery. The sensor is responsible for the translation of physical phenomena detected/measured in the RoI to electrical signals. The transceiver enables the SN to communicate wirelessly with its neighboring SNs and with the sink node. The processor is responsible for performing all required computations and controlling both the sensor and transceiver. The battery supplies all three components with power. The type and capacity of the SN battery is carefully chosen according to the application and the required mission time of the WSN

(<http://www.sensorsmag.com/components/a-practical-guide-to-battery-technologies-for-wireless-sensor-networking>).

Each of these components is subject to random failure [6], [23] due to several reasons such as faulty hardware, faulty software, harsh environmental conditions, and degradation with time. Accordingly, each of the SN's four main components has a given reliability or, alternatively, a probability of failure during the WSN mission time T_m as defined in Section 3.1. As mentioned earlier in Section 3, the reliabilities of the different components of an SN can be estimated through a standard reliability prediction test provided by the SN vendor or through reliability testing techniques [5].

Since each of the four components can either function or fail, i.e., be in an *on* or *off* state, an SN can theoretically have 2^4 possible states. To describe these states, let the binary variables x_s , x_t , x_p , and x_b be the state indicators of the sensor, transceiver, processor, and battery, respectively, of an SN as defined in (2). Hence, an SN state x is described using a tuple of these four variables $\{x_s, x_t, x_p, x_b\}$. These variables are not statistically independent; the sensor and transceiver cannot possibly function if either the processor or the battery fails. Therefore, some of the SN states are practically impossible, and hence, their probability of occurrence is zero.

To calculate the probability of occurrence of the other possible states, let λ_s , λ_t , λ_p , and λ_b be the probabilities of failure of the sensor, transceiver, processor, and battery, respectively. It should be noted that the estimated probability of failure for any given device or hardware component is obtained regardless of the failure of any other device or component. Hence, λ_s and λ_t are actually the probability of failure of the sensor and transceiver conditioned on the event that the component is properly controlled (i.e., processor is functional) and powered (i.e., battery is functional). Similarly, λ_p is the probability of failure of the processor conditioned on the event that the battery is functional, where as λ_b is the unconditional probability that the SN power unit or battery fails during T_m . According to the above definitions, the probability of an SN state can be given by the following equations:

$$\begin{aligned} \text{Prob}(x) &= \text{Prob}(x_s, x_t, x_p, x_b) \\ &= \text{Prob}(x_s, x_t | x_p, x_b) \cdot \text{Prob}(x_p, x_b) \\ &= \text{Prob}(x_s | x_p, x_b) \cdot \text{Prob}(x_t | x_p, x_b) \cdot \text{Prob}(x_p | x_b) \cdot \text{Prob}(x_b) \end{aligned} \quad (8)$$

Equation (8) makes use of the fact that the states of the sensor and the transceiver are independent when conditioned on the states of the processor and battery. Figure 2 illustrates the SN's states which have a non-zero

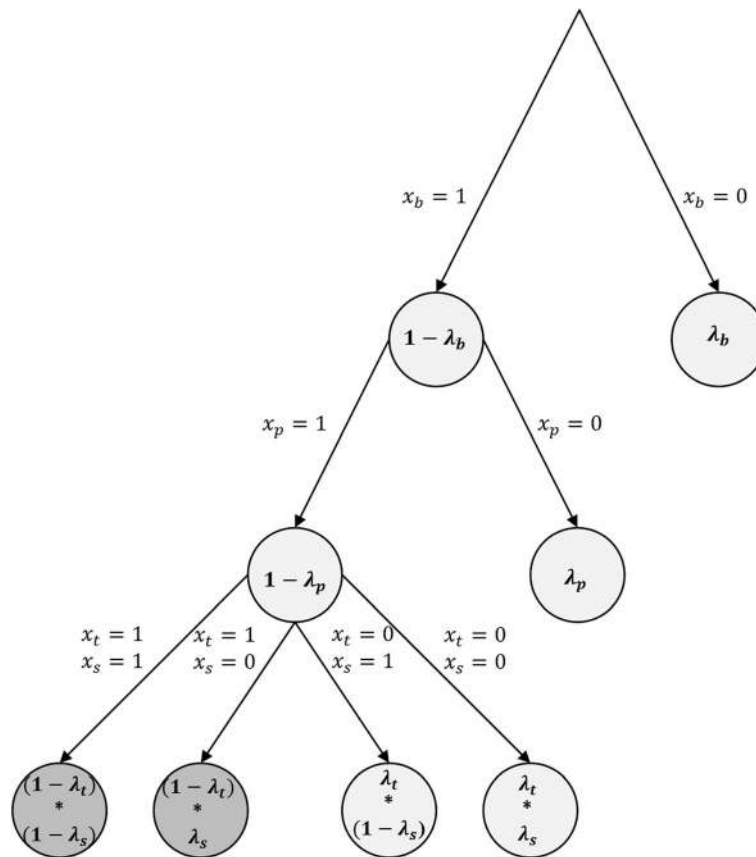


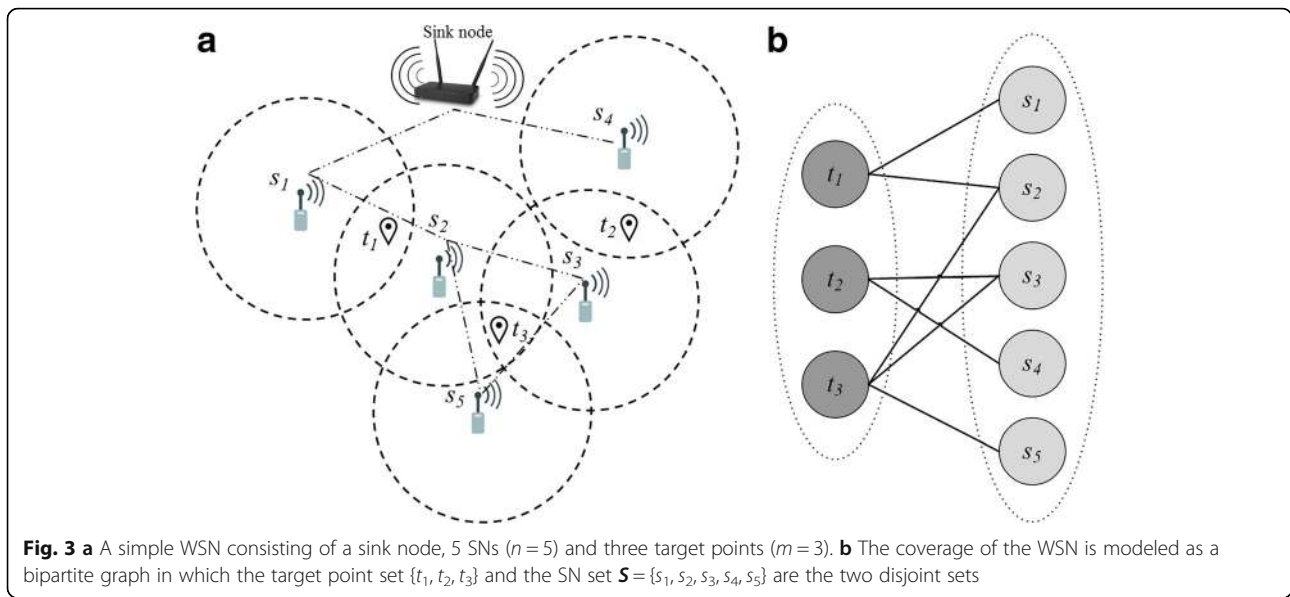
Fig. 2 SN states: the paths from the top node to a bottom node correspond to the SN states with non-zero probability. The probability of a path, i.e., the probability of a state, is the product of the probabilities in the associated transitions. The SN states corresponding to the *relay* mode and the *on* mode are both marked by a dark shade of gray

probability. It is straightforward to verify that the sum of the probabilities of these states is equal to unity. There are two SN states at which the SN is of use to the WSN. The first state is described by the tuple $\{1,1,1,1\}$, at which all four components are functional and the SN can both sense its surroundings and communicate wirelessly. This state corresponds to the *on* mode of operation in which the SN is fully functional as defined in Section 1. The second state is described by the tuple $\{0,1,1,1\}$ at which only the sensor(s) failed and the SN can only communicate wirelessly, i.e., acts as a relay node. This state corresponds to the *relay* mode of operation in which the SN is partially functional as defined in Section 1. In all the practically possible remaining states, the SN does not serve the network, and hence, a SN in these states is considered to be in the *off* mode of operation.

4.2 Wireless sensor network model

We assume that the targeted RoI of the WSN is a two-dimensional area in which there is a finite set of locations

that require some form of monitoring (e.g., motion, image, video) using static SNs. These locations are called *target points* and are denoted by the set $T = \{t_j\}$ for $j = 1, \dots, m$. To maintain generality, we do not assume that the target points conform to any regular pattern. Target points are monitored by the SNs in the WSN. We assume that the SNs used in the deployment of the WSN can be of different types (e.g., sound, image) and can have different coverage profiles (e.g., binary disk model, field of view (FoV) model), i.e., the WSN can be heterogeneous in nature. Let the set of deployed SNs be denoted by $S = \{s_i\}, i = 1, \dots, n$. We assume an arbitrary deployment configuration in which an SN can monitor multiple target points. We also assume that a target point can be monitored by more than one SN. Therefore, in terms of coverage, the WSN can be modeled as a bipartite graph. Figure 3 shows an example of a WSN consisting of 5 SNs ($n = 5$) monitoring three target points ($m = 3$) and the resulting bipartite graph representation of the network coverage, assuming SNs are characterized by a binary disk coverage model. All



sensory data acquired by the SNs should be relayed to a sink node with an arbitrary fixed position in the RoI through wireless multi-hop communications. We assume that all deployed SNs have a fixed communication range, r_c . Hence, any two SNs deployed have a wireless communication link if the distance between them is less than or equal to r_c . Naturally, it is required that the WSN remains functional in terms of coverage and connectivity throughout its intended mission time T_m . To express this mathematically, we use the following definition:

Definition: A WSN is said to be functional in terms of both coverage and connectivity if both of the following two conditions are met:

1. Each target point t_j for $j = 1, \dots, m$ is covered by at least one SN with an uncompromised sensing capability, i.e., an SN in the *on* state. Let the set Y_j be the set of SNs in the *on* state that monitor t_j . Then this condition can be expressed as, $|Y_j| \neq 0, \forall j = 1, \dots, m$ where $|\cdot|$ denotes the size of a set.
2. Within each Y_j there is at least one SN that has at least one functional path to the sink node. This implies that SNs along that path, including the source SN, have uncompromised communication capabilities, i.e., in either the *on* or the *relay* state. Hence, the events detected at any t_j can be relayed back to the sink node. Let the set Z_j be the set of SNs which belong to Y_j that are connected to the sink node. Hence, $Z_j \subseteq Y_j$. The condition can be expressed as $|Z_j| \neq 0, \forall j = 1, \dots, m$.

In the next subsection, we will use the above definition of WSN functionality conditions in defining the structure function of the WSN, which we defined in Section 3.2.

4.3 Wireless sensor network reliability metric derivation

The reliability of the WSN, \mathbf{S} , denoted by $R(\mathbf{S})$, is defined as the probability that the WSN remains functional, in terms of coverage and connectivity, subject to four types of SN component failures during its intended mission time, T_m . In order to use the combinatorial approach outlined in Section 3.2 to derive $R(\mathbf{S})$, we must define the states of \mathbf{S} and its structure function. To define the states of \mathbf{S} , let $X_s, X_t, X_p,$ and X_b be the subsets of SNs in \mathbf{S} that have failed sensors, transceivers, processors, and batteries, respectively. Hence, a state of the WSN \mathbf{S} is described by the tuple $\pi \equiv \{X_s, X_t, X_p, X_b\}$, where $X_s, X_t, X_p, X_b \subseteq \mathbf{S}$. Therefore, each state π is associated with a unique combination of SN components' failures. To calculate the probability of occurrence of a given state, π , the corresponding state $x_i(\pi)$ of each individual SN $s_i \in \mathbf{S}$ must be identified. Assuming the components belonging to different SNs fail independently, $Prob(\pi)$ can be expressed by:

$$\begin{aligned}
 Prob(\pi) &= Prob(X_s, X_t, X_p, X_b) \\
 &= \prod_{i=1}^N Prob(x_i(\pi))
 \end{aligned} \tag{9}$$

Table 1 lists the different values of the probability of an individual SN state $x_i(\pi)$ for a given network state π based on the SN states illustrated in Fig. 2. The first state in Table 1 corresponds to a SN in the *on* mode, the ninth state corresponds to the *relay* mode, while the rest of the non-zero probability states correspond to the *off* mode as illustrated in Fig. 2.

As defined in Section 3.2, the structure function of a system is a binary indicator of whether the system is functional at a given state. For a WSN, \mathbf{S} , the structure function indicates whether the network can maintain

Table 1 Evaluation of the probability of the corresponding individual SN states for a given WSN state= $\mathbf{X}_s, \mathbf{X}_t, \mathbf{X}_p, \mathbf{X}_b$, where “true” and “false” are denoted by 1 and 0, respectively, and $\lambda_s^i, \lambda_t^i, \lambda_p^i, \lambda_b^i$ are the probabilities of failure of the four main components of SN s_j

$s_j \in X_s$	$s_j \in X_t$	$s_j \in X_p$	$s_j \in X_b$	Prob($x_i(\pi)$)
0	0	0	0	$(1 - \lambda_s^i) (1 - \lambda_t^i) (1 - \lambda_p^i) (1 - \lambda_b^i)$
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	$(1 - \lambda_s^i) \lambda_t^i (1 - \lambda_p^i) (1 - \lambda_b^i)$
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	$\lambda_s^i (1 - \lambda_t^i) (1 - \lambda_p^i) (1 - \lambda_b^i)$
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	$\lambda_s^i \lambda_t^i (1 - \lambda_p^i) (1 - \lambda_b^i)$
1	1	0	1	0
1	1	1	0	$\lambda_p^i (1 - \lambda_b^i)$
1	1	1	1	λ_b^i

its functionality conditions in terms of both coverage and connectivity under a specific combination of SNs components failures. Let Π be the set of all possible states of \mathbf{S} . Based on the definition provided in the previous subsection, the structure function of \mathbf{S} can be expressed as follows:

$$f(\boldsymbol{\pi}) = \begin{cases} 1, & \text{if } \mathbf{Z}_j \subseteq \mathbf{Y}_j \neq \phi \quad \forall j = 1, \dots, m \\ 0, & \text{otherwise} \end{cases} \quad (10)$$

Similar to (3), we can now express the reliability of the WSN \mathbf{S} as follows:

$$R(\mathbf{S}) = \text{Prob}(\mathbf{S} \text{ is functional during } T_m) = \sum_{\boldsymbol{\pi} \in \Pi} [f(\boldsymbol{\pi}) \cdot \text{Prob}(\boldsymbol{\pi})] \\ = \sum_{X_s \subseteq \mathbf{S}} \sum_{X_t \subseteq \mathbf{S}} \sum_{X_p \subseteq \mathbf{S}} \sum_{X_b \subseteq \mathbf{S}} [f(X_s, X_t, X_p, X_b) \cdot \prod_{i=1}^N \text{Prob}(x_i(\boldsymbol{\pi}))] \quad (11)$$

Equation (11) states that the reliability of the WSN is the summation of all the probabilities of the WSN states that have a structure function value of unity (i.e., the probabilities of all the paths of the WSN \mathbf{S}). Depending on the set of failed components in the state $\boldsymbol{\pi}$, the individual probabilities $\text{Prob}(x_i(\boldsymbol{\pi}))$, $i = 1, \dots, N$ can be calculated using Table 1.

5 Reliability metric calculation

From the derived expression of $R(\mathbf{S})$ in (11), it is clear that the reliability calculation involves in turn evaluating

the structure function of the network, $f(\boldsymbol{\pi})$, for all possible states of \mathbf{S} , i.e. for all $\boldsymbol{\pi} \in \Pi$. As explained in Section 3.2, this can pose a computational challenge since WSNs designed for practical purposes are often composed of tens of SNs, resulting in a huge number of possible network states. This problem is further complicated by modeling the SNs as four-component systems which in turn have multiple possible states. For example, a WSN composed of just 30 SNs would have $2^{4 \cdot 30} = 2^{120}$ states. This means that the calculation of the reliability metric in this case would require a prohibitive amount of time. To solve this computational problem, we make use of the following two properties of the WSN, \mathbf{S} , using the model presented in Section 4.2:

- The majority of the network states have null probabilities, and hence, they do not contribute to the value of $R(\mathbf{S})$. This stems from the fact the majority of the individual SN states also have a null probability (i.e., are not practically possible) as shown in Table 1.
- The WSN \mathbf{S} has the property of being a monotone/coherent system [21]. This property implies the following. If the failure of a set of SNs' components causes \mathbf{S} to fail, then the failure of any set which contains this set will also cause \mathbf{S} to fail. For example, if we assume that the SNs s_1 and s_2 in the WSN depicted in Fig. 3a are both in the *off* mode while the remaining SNs are in the *on* mode, then it

can be readily observed that this would cause \mathcal{S} to fail since any phenomenon at target point t_1 cannot be detected or communicated to the sink node. This means that network states corresponding to this situation have a structure function value of zero as expressed in (10). Using the monotone property, we can say that the network states that include the SNs s_1 and s_2 being in the *off* mode and s_4 being in the *relay* mode would also have a structure function value of zero without actually evaluating the function.

These two useful properties are used to develop a Breadth-First Search (BFS) algorithm that generates the complete path set of \mathcal{S} , denoted by Π_1 , and use it to calculate $R(\mathcal{S})$ using (11). The general structure of the developed search algorithm is illustrated in Fig. 4. The pseudo-code of the algorithm, which provides execution

details, is given in Table 2. The structure of the algorithm can be summarized in the following steps. In step 1, all the required parameters for the calculation of $R(\mathcal{S})$ are specified as inputs. This includes the two-dimensional RoI layout, the positions of the target locations within the RoI provided by the set of target points $T = \{t_j\}$, the positions of the deployed SNs provided by $\mathcal{S} = \{s_i\}$, the types of the deployed SNs including their coverage profiles and wireless communication ranges, and the probabilities of failure of the SN components associated with each SN type. We assume here that the sink node can be at any fixed arbitrary position in the targeted RoI. We initialize the value of $R(\mathcal{S})$ with the probability of the network state π which corresponds to all the deployed SNs being in the on mode. Since this network state is an obvious path of \mathcal{S} , we also initialize the network path set Π_1 with this state as expressed in 1.c. in Table 2.

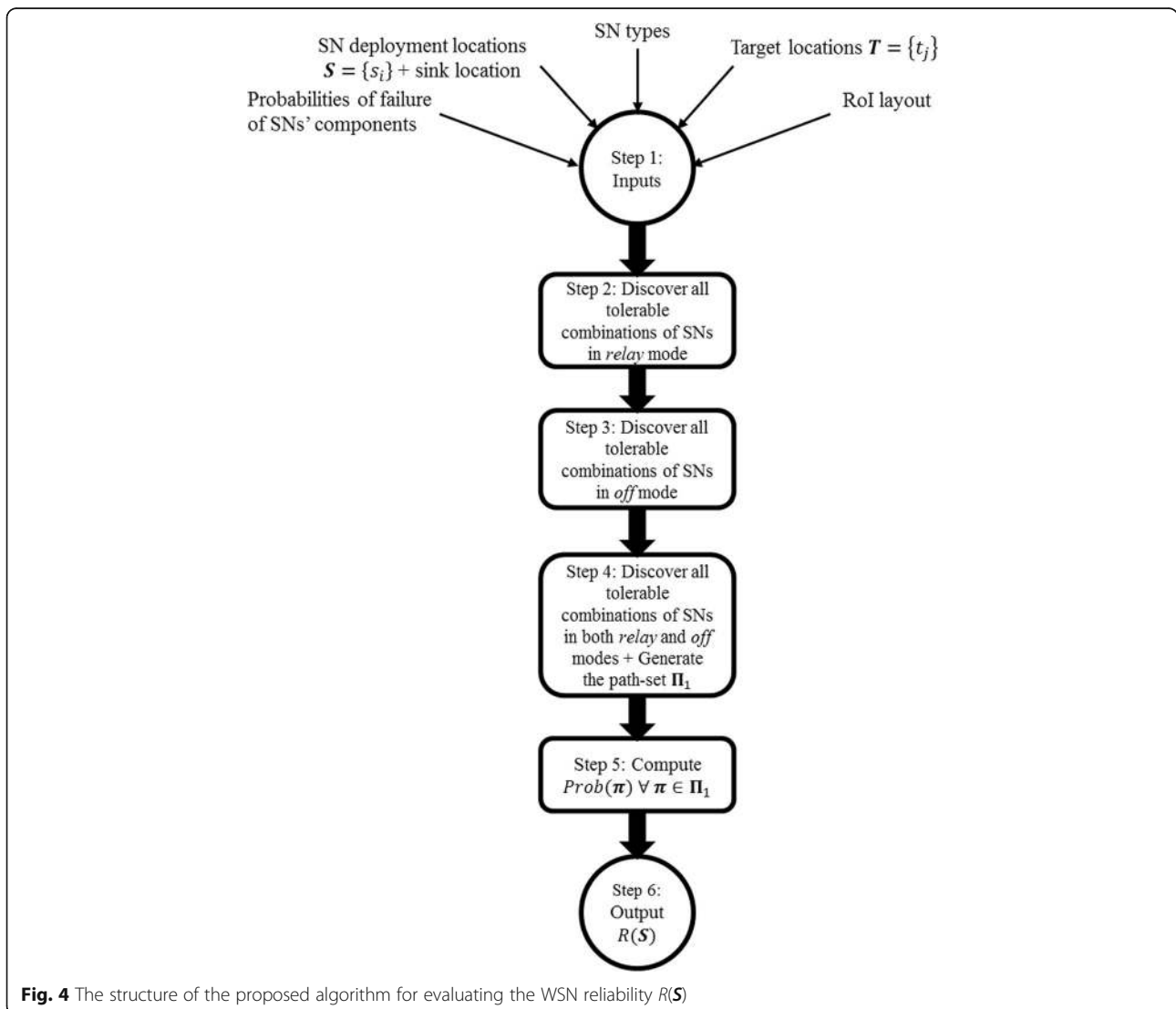


Fig. 4 The structure of the proposed algorithm for evaluating the WSN reliability $R(\mathcal{S})$

Table 2 Pseudo-code for the proposed algorithm for calculating the reliability of a WSN S

Step	Algorithm for computing WSN reliability $R(S)$
1.a.	Set all parameters ($\mathbf{S} = \{s_i\}$, $\mathbf{T} = \{t_j\}$, types of SNs, sink location, λ_s^i , λ_t^j , λ_p^i and λ_o^j for $i = 1, \dots, n$ and $j = 1, \dots, m$)
1.b.	Initialize $R = \text{Prob}(\boldsymbol{\pi} s_i \in \mathbf{S} \text{ is in on mode } \forall i = 1, \dots, n)$
1.c.	Initialize $\boldsymbol{\pi}_1 = \{\{\boldsymbol{\pi} s_i \in \mathbf{S} \text{ is in on mode } \forall i = 1, \dots, n\}\}$
2.a.	Let k be the number of SNs in <i>relay</i> mode. Initialize $k = 1$.
2.b.	Let \mathcal{F}_r^k be a k -combination of SNs in <i>relay</i> mode. Let \mathbf{F}_r^k be the set of k -combinations of SNs in <i>relay</i> mode that \mathbf{S} can tolerate. Initialize $\mathcal{F}_r^k = \mathbf{F}_r^k = \{\emptyset\}$.
2.c.	For $i = 1, \dots, n$ - Let s_i be in <i>relay</i> mode, i.e. $\mathcal{F}_r^k = \{s_i\}$ - Evaluate $f(\boldsymbol{\pi} \mathcal{F}_r^k)$ using (10) - If $f(\boldsymbol{\pi} \mathcal{F}_r^k) = 1 \rightarrow \mathbf{F}_r^k = \mathbf{F}_r^k \cup \mathcal{F}_r^k$ End For loop
2.d.	While $\mathbf{F}_r^k \neq \{\emptyset\} \rightarrow k = k + 1$, Let $F_{r^{k-1}} \in \mathbf{F}_r^{k-1}$, $\mathcal{F}_r^k = \mathbf{F}_r^k = \{\emptyset\}$
2.e.	For $l = 1, \dots, \mathbf{F}_r^{k-1} $ and $i = 1, \dots, n$ - Let $\mathcal{F}_r^k = \{F_{r^{k-1}}, s_i\}$ - Evaluate $f(\boldsymbol{\pi} \mathcal{F}_r^k)$ using (10) - If $f(\boldsymbol{\pi} \mathcal{F}_r^k) = 1 \rightarrow \mathbf{F}_r^k = \mathbf{F}_r^k \cup \mathcal{F}_r^k$
2.f.	End For loops, End While loop
3.a.	Let k be the number of SNs in <i>off</i> mode. Initialize $k = 1$.
3.b.	Let \mathcal{F}_o^k be a k -combination of SNs in <i>off</i> mode. Let \mathbf{F}_o^k be the set of k -combinations of SNs in <i>off</i> mode that \mathbf{S} can tolerate. Initialize $\mathcal{F}_o^k = \mathbf{F}_o^k = \{\emptyset\}$.
3.c.	Repeat step 2.c. for <i>off</i> mode, i.e. $\mathcal{F}_o^k = \{s_i\}$
3.d.	While $\mathbf{F}_o^k \neq \{\emptyset\} \rightarrow k = k + 1$, Let $F_{o^{k-1}} \in \mathbf{F}_o^{k-1}$, $\mathcal{F}_o^k = \mathbf{F}_o^k = \{\emptyset\}$
3.e.	Repeat 2.e. using $F_{o^{k-1}}$ and \mathcal{F}_o^k to get \mathbf{F}_o^k
3.f.	End For loops, End While loop
4.a.	Let \mathcal{F}_r and \mathcal{F}_o be a combination of SNs in <i>relay</i> and <i>off</i> modes respectively. Let \mathbf{F}_r and \mathbf{F}_o be the sets of all combinations of SNs of in <i>relay</i> and <i>off</i> mode that that \mathbf{S} can tolerate respectively. Let $F_{r_l} \in \mathbf{F}_r$ and $F_{o_{l_o}} \in \mathbf{F}_o$
4.b.	For $l_r = 1, \dots, \mathbf{F}_r $ and $l_o = 1, \dots, \mathbf{F}_o $ - Let $\mathcal{F}_r = F_{r_l}$ and $\mathcal{F}_o = F_{o_{l_o}}$ - Evaluate $f(\boldsymbol{\pi} \mathcal{F}_r, \mathcal{F}_o)$ using (10) - If $f(\boldsymbol{\pi} \mathcal{F}_r, \mathcal{F}_o) = 1 \rightarrow \boldsymbol{\pi}_1 = \boldsymbol{\pi}_1 \cup \boldsymbol{\pi}$ End For loops
5.a.	Let $\boldsymbol{\pi}_l \in \boldsymbol{\pi}_1$
5.b.	For $l = 1, \dots, \boldsymbol{\pi}_1 $ - $R(\mathbf{S}) = R(\mathbf{S}) + \text{Prob}(\boldsymbol{\pi}_l)$ End For loop
6.	Output: $R(\mathbf{S})$

Whether any other given state $\boldsymbol{\pi}$ is a path of the network or not (i.e., whether $f(\boldsymbol{\pi}) = 1$ or 0) depends on the WSN configuration/topology. To evaluate $f(\boldsymbol{\pi})$, the two conditions of WSN functionality, namely, coverage and connectivity, are checked according to the same definitions and order presented in Section 4.2. Checking the WSN coverage is straightforward and has the computational complexity of $O(n^*m)$. If one or more of the target points in the RoI is uncovered, then $f(\boldsymbol{\pi}) = 0$ and the

connectivity condition does not need to be checked. Checking the WSN connectivity condition is more complex computationally, and it depends on the connectivity matrix between the SNs and the sink. Constructing that matrix has the complexity $O(n^2)$. For every WSN state $\boldsymbol{\pi}$, the connectivity matrix is updated according to SNs' modes in the state $\boldsymbol{\pi}$ and the updated connectivity matrix is used to check the connectivity condition. We carry out this check using the Floyd-

Warshall algorithm (https://en.wikipedia.org/wiki/Floyd%E2%80%93Warshall_algorithm), which can compute the shortest paths (if one exists) between all SNs (in the *on* or *relay* mode) and the sink node with the computational complexity $O(n^3)$. If all the SNs covering any given target point do not have a path to the sink node, $f(\pi) = 0$, otherwise connectivity is intact and $f(\pi) = 1$.

In step 2, the algorithm searches for all the combinations of SNs that can be in the *relay* mode without compromising the functionality of \mathcal{S} , assuming the remainder of the deployed SNs are in the *on* mode. These SN combinations are referred to as the “tolerable combinations of SNs in the *relay* mode.” This means that for the network states corresponding to these SN combinations, the structure function $f(\pi)$ expressed in (10) is equal to unity. To perform the required search in step 2, we define F_r^k as the set that holds the tolerable combinations of SNs in *relay* mode of length k starting with $k=1$ as expressed in 2.a–2.c. in Table 2. For example, consider the WSN depicted in Fig. 3a. The set of single tolerable SNs in the *relay* mode will be given by $F_r^1 = \{ \{s_1\}, \{s_2\}, \{s_3\}, \{s_4\}, \{s_5\} \}$. The algorithm then proceeds with the search for an increasing value of k as expressed in 2.d–2.f. in Table 2. For example, the combination $\{s_1, s_3\}$ belongs to F_r^2 while $\{s_1, s_2\}$ does not. This search continues until the algorithm reaches a value of k which results in an empty F_r^k , i.e., $F_r^k = \{\emptyset\}$. The set of all tolerable combinations of different lengths of SNs in *relay* mode is denoted F_r .

In step 3, the algorithm searches for all the combinations of SNs that can be in the *off* mode without compromising the functionality of \mathcal{S} , assuming the remainder of the SNs is in the *on* mode, i.e. tolerable combinations of SNs in the *off* mode. The search follows the same procedure in step 2. We define F_o^k as the set that holds the tolerable combinations of SNs in the *off* mode of length k . Using the same example WSN in Fig. 3a, $F_o^1 = \{ \{s_2\}, \{s_3\}, \{s_4\}, \{s_5\} \}$. The combination $\{s_4, s_5\}$ belongs to F_o^2 while $\{s_2, s_5\}$ does not. The set of all tolerable combinations of different lengths of SNs in the *off* mode is denoted F_o .

In step 4, the algorithm uses the sets F_r and F_o to discover all the pairs of combinations of SNs that can be in the *relay* and *off* modes simultaneously without compromising the functionality of \mathcal{S} , assuming the remainder of the SNs is in the *on* mode. For example, the combination $\{s_1, s_3\}$ can be in the *relay* mode while $\{s_5\}$ can be in the *off* mode simultaneously without causing the WSN depicted in Fig. 3a to fail. Each of the discovered pairs of combinations corresponds to one or more distinct network path and hence the complete path set Π_1 is updated accordingly as expressed in 4.b in Table 2. In step 5, the probabilities of the network paths in Π_1

are calculated using (11) and Table 1. Finally, the reliability of the given WSN $R(\mathcal{S})$ is calculated using (7) and given as an output in step 6.

6 Case study

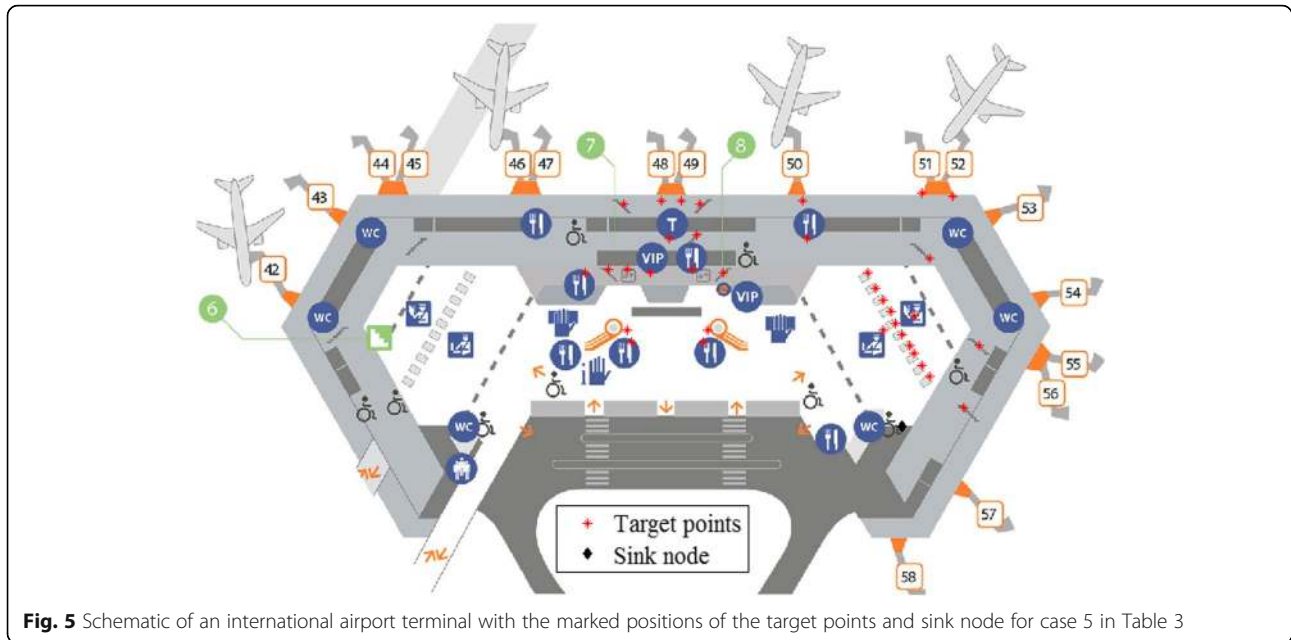
6.1 Experimental setup

In this section, we apply the reliability metric that we proposed in Section 4 and the search algorithm proposed in Section 5 to evaluate the reliability of a surveillance WSN designed to cover part of an international airport terminal (http://www.aeroflot.ru/cms/en/before_and_after_fly/terminal_info), which comprises the RoI of the WSN. Target points, marked on the figure in red, represent the vital locations that need to be placed under image/video surveillance such as arrival checkpoints, entrances, and staircases. The sink node to which all SNs in the WSN should be connected is marked in black.

To obtain our test deployments of the WSN, we use the Variable Length Genetic Algorithm (VLGA) presented in [24]. This optimization algorithm is designed to obtain cost-optimized deployments for heterogeneous WSNs that fulfill specific design objectives using a variable-length chromosome integer-encoded GA. In [24], the only considered design objective is providing coverage for all the target points in the RoI, i.e., providing full-coverage of the set $T = \{t_j\}$ for $j = 1, \dots, m$. However, since a well-designed surveillance WSN should be functional in terms of coverage and connectivity, as defined in Section 3.2, we modified the VLGA in [24] to add network connectivity to the design objectives. To achieve this, we modify the fitness function that is used to evaluate the fitness of the candidate deployments or chromosomes in [24], as follows:

$$f(c(l)) = - \left(\sum_{i=1}^l p_i + w_1 * (m - \text{cov}) + w_2 * \text{con_test} \right) \quad (12)$$

where $\sum_{i=1}^l p_i$ is the total cost of the deployment $c(l)$, cov is the number of target points that are covered by $c(l)$, con_test is a binary variable that is equal to unity when $c(l)$ is a disconnected deployment (i.e., has isolated SNs from the sink node) and zero otherwise, w_1 is the penalty imposed on the fitness for failing to cover a single target point and w_2 is a penalty for violating the connectivity constraint. The negative sign is added so that the maximum fitness would correspond to deployments achieving the coverage and connectivity constraints at minimum cost. For further details on the VLGA and the settings of its parameters, we refer the reader to the study in [24]. Both the VLGA and the search algorithm presented in Section 5 for the reliability metric calculation were implemented using MATLAB version 7.8.0



which runs on an Intel processor Core i7-3621QM CPU, 2.1 GHz and 6 GB of RAM.

To demonstrate the proposed metric ability to evaluate the reliability of heterogeneous deployments, we assume that there are two types of SNs available for the deployment of the WSN. The coverage profile parameters and probabilities of failure of the SNs' components for each SN type are listed in Table 3. We assume that both SN types have a coverage range and a communication range of 30 and 40 m, respectively. Although the exact reliability figures for commercial SNs such as Tmote2 and Iris nodes are not publicly available, we estimated the given probabilities of failure using the reliability figures available for Texas Instrument CC2420 IEEE 802.15.4 transceiver (<http://www.ti.com/product/CC2420/quality>) as a reference point, assuming a WSN mission time of 5 years. We also used the fact that sensor hardware is the SN component most prone to failure [6] and that the premature battery failure rate for the highly durable lithium thionyl chloride batteries recently used for SNs is very low (https://www.omnisen.com/oms_cds/media/008-002-002%20OmniSense%20FMS%20Sensor%20Battery%20Life.pdf).

To thoroughly evaluate the proposed metric in terms of the computational efficiency, it is crucial to assess the effect of the deployment size and complete path set

size $|\Pi_1|$ for a given deployment on the computation time of the proposed algorithm outlined in Table 2. To achieve this objective, we apply the VLGA to obtain cost-optimized deployments for five target point sets of sizes $m = 15, 20, 25, 30,$ and 35 . For each deployment scenario, i.e., for each value of m , we obtain five deployments of different sizes (i.e., different values of n), with the deployment of the smallest size being the most cost-optimal and the deployment with the largest size being the least cost-optimal. Each deployment fulfills the coverage and connectivity network functionality conditions in the case of no SN failures and has a different level of SN redundancy, where the higher the n , the higher the redundancy level and the larger the complete path set Π_1 and vice versa. Data of the resulting 25 deployments, including the size of the deployment (n), number of SNs of each type (n_1 and n_2), and the total deployment cost (C), are presented in Table 4.

6.2 Results and discussion

To evaluate the computational efficiency of the proposed algorithm outlined in Table 2, we use the algorithm to evaluate the reliability of the WSN deployments in Table 4. For each deployment, Table 4 shows the value of the reliability $R(S)$, the total number of possible network states $|\Pi|$ (which

Table 3 Parameters of the SN types used in the deployment of the case-study surveillance WSN

	FoV	r_s	r_c	λ_s	λ_r	λ_p	λ_b	Price(\$)
Type 1	90°	30 m	40 m	1.0×10^{-2}	5.0×10^{-3}	2.0×10^{-3}	1.0×10^{-3}	150
Type 2	60°	30 m	40 m	1.5×10^{-2}	5.5×10^{-3}	2.5×10^{-3}	1.5×10^{-3}	100

Table 4 Data of the obtained deployments for the case-study surveillance WSN for the RoI shown in Fig. 5

Deployment no.	n	n_1	n_2	C (\$)	$R(S)$	$ \Pi $	$ \Pi_1 $	FE	$FE/ \Pi $ (%)	
Scenario 1 $m = 15$	S1-D1	9	0	9	900	0.829	2^{36}	4	45	6.55×10^{-8}
	S1-D2	10	1	9	1050	0.849	2^{40}	28	164	1.49×10^{-8}
	S1-D3	11	2	9	1200	0.870	2^{44}	196	723	4.11×10^{-9}
	S1-D4	12	3	9	1350	0.891	2^{48}	1.37×10^3	4.16×10^3	1.48×10^{-9}
	S1-D5	13	4	9	1500	0.912	2^{52}	9.60×10^3	3.01×10^3	6.68×10^{-10}
Scenario 2 $m = 20$	S2-D1	16	3	13	1750	0.731	2^{64}	16	256	1.39×10^{-15}
	S2-D2	17	4	13	1900	0.748	2^{68}	112	881	2.98×10^{-16}
	S2-D3	18	4	14	2000	0.756	2^{72}	560	3.08×10^3	6.52×10^{-17}
	S2-D4	19	5	14	2150	0.774	2^{76}	3.92×10^3	1.46×10^4	1.93×10^{-17}
	S2-D5	20	6	14	2300	0.793	2^{80}	2.74×10^4	9.08×10^4	7.51×10^{-18}
Scenario 3 $m = 25$	S3-D1	21	1	20	2150	0.657	2^{84}	64	1.24×10^3	6.40×10^{-21}
	S3-D2	22	2	20	2300	0.673	2^{88}	448	4.16×10^3	1.34×10^{-21}
	S3-D3	23	3	20	2450	0.696	2^{92}	5.38×10^3	1.97×10^4	3.98×10^{-22}
	S3-D4	24	4	20	2600	0.703	2^{96}	3.23×10^4	7.49×10^4	9.45×10^{-23}
	S3-D5	25	5	20	2750	0.720	2^{100}	2.26×10^5	5.37×10^5	4.24×10^{-23}
Scenario 4 $m = 30$	S4-D1	25	8	17	2900	0.630	2^{100}	128	2.91×10^3	2.29×10^{-25}
	S4-D2	26	6	20	2900	0.612	2^{104}	192	4.51×10^3	2.22×10^{-26}
	S4-D3	27	6	21	3000	0.633	2^{108}	2.30×10^3	1.61×10^4	4.95×10^{-27}
	S4-D4	28	7	21	3150	0.649	2^{112}	1.61×10^4	6.61×10^4	1.27×10^{-27}
	S4-D5	29	8	21	3300	0.665	2^{116}	1.13×10^5	3.55×10^5	4.28×10^{-28}
Scenario 5 $m = 35$	S5-D1	28	4	24	3000	0.553	2^{112}	32	876	1.69×10^{-29}
	S5-D2	29	6	23	3200	0.555	2^{116}	48	1.34×10^3	1.61×10^{-30}
	S5-D3	30	7	23	3350	0.568	2^{120}	336	4.36×10^3	3.28×10^{-30}
	S5-D4	31	8	23	3500	0.589	2^{124}	6.38×10^3	3.04×10^4	1.43×10^{-31}
	S5-D5	32	9	23	3650	0.597	2^{128}	4.47×10^4	1.57×10^5	4.61×10^{-32}

is equal to $2^{4 \cdot n}$, the size of the deployment complete path set $|\Pi_1|$, the number of network structure function evaluations FE performed by the algorithm, and the value of the ratio $FE/|\Pi_1|$ in percentage points. The latter ratio is used as a measure of the computational efficiency of the proposed algorithm. This is because the most computationally expensive sub-routine in the algorithm is the evaluation of the network structure function expressed in (10). For each structure function evaluation, checking the two network functionality conditions, i.e., checking the network coverage of the set of target points and the connectivity to the sink, has a computational complexity of $O(n \cdot m)$ and $O(n^3)$, respectively. Therefore, the computation time of the algorithm is mainly determined by the number of structure function evaluations denoted by FE .

It can be readily observed that the values of $R(S)$, $|\Pi_1|$, and FE increase steadily with the increase of n in each deployment scenario. This behavior is expected and is attributed to the increase in the level of SN redundancy in the deployment as n increases. An increase in the level of SN redundancy translates to an exponential

increase in the number of the paths of the deployment and hence the increase of the reliability $R(S)$. It can also be observed that the number of performed structure function evaluations FE increases significantly with the increase in the level of SN redundancy as a direct result of the exponential increase in $|\Pi_1|$. However, the value of the ratio $FE/|\Pi_1|$ decreases rapidly with the increase of n in each scenario. It can also be observed that the ratio $|\Pi_1|/FE$ generally increases with the increase of the level of SN redundancy in each of the five tested scenarios. For example, the value of $|\Pi_1|/FE$ is 27% for the deployment S3-D3 and 43% for S3-D4. These two observations mean that the computational efficiency of the proposed algorithm becomes more prominent with the increase of the SN redundancy level due to the efficiency of its search method for the deployment's paths performed by the algorithm.

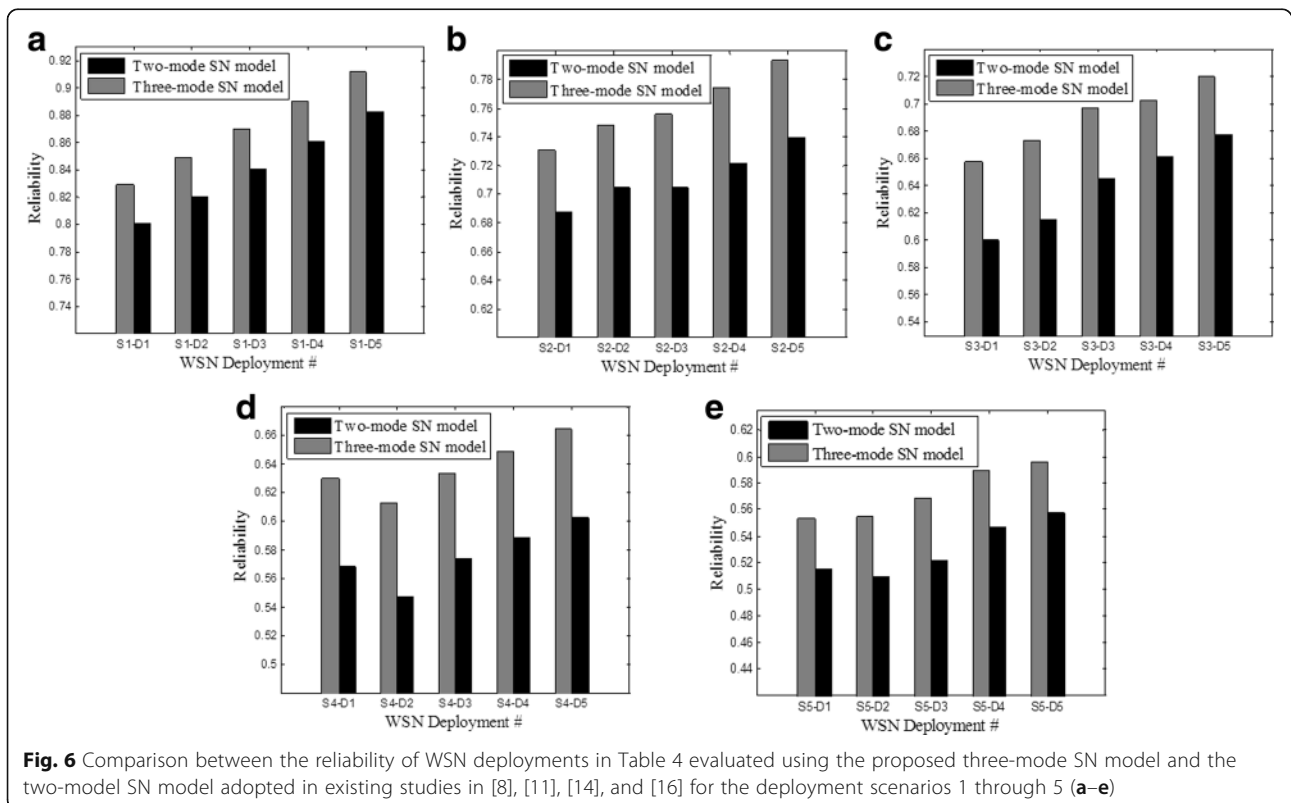
It is instructive to examine the two deployments S4-D1 and S4-D2 which are the only exception in Table 4 to the trend discussed above. Although S4-D2 has more SNs than S4-D1 and a larger number of paths $|\Pi_1|$, it is

approximately 2% less reliable than S4-D1. This can be attributed to the higher ratio of more reliable SNs of type 1 to the less reliable SNs of type 2 in the S4-D1 compared to S4-D2. It can also be observed that depends mainly on the SN redundancy level (i.e., the value of $|\Pi_1|$) relative to the total number of deployed SNs n (which controls the value of the probability of occurrence of the paths in Π_1). Since the increase in n in each deployment scenario is very similar, the value of $|\Pi_1|$ for the deployments of the same order in the different scenarios (e.g., S4-D3 and S5-D3) is comparable. This means that the SN redundancy level relative to n actually decreases with the increase of deployment scenario order, i.e., with the increase of m , resulting in a steady decrease in $R(S)$.

To demonstrate the significance of modeling the SNs as three-mode (*on*, *relay*, and *off*) devices, we evaluate the reliability of the deployments presented in Table 4 using the reliability metric proposed in [16], which adopts the conventional two-mode (*on* and *off*) SN model. For a fair comparison, we use our proposed network structure function expressed in (10) (which defines the WSN functionality in terms of both network coverage and connectivity as opposed to network coverage only in [16]). Since the two-mode SN model assumes that a given SN is either in a fully functional (*on* state)

or failed (*off* state) state, SNs cannot contribute to the network functionality as relays. Hence, the corresponding probability of the *off* state for a given SN s_i is equal to the probability that any of the four SN components fail, i.e., is equal to unity minus the probability that all of the four SN components are functioning simultaneously (i.e., $1 - (1 - \lambda_s^i) (1 - \lambda_r^i) (1 - \lambda_p^i) (1 - \lambda_t^i)$).

As can be observed from Fig. 6, the value of $R(S)$ evaluated using the two-mode SN model is significantly smaller than that using the proposed three-mode model for all the deployments in Table 4, exceeding 6% for some deployments. This behavior is expected and can be attributed to the fact that the two-mode SN model is an unrealistic model that does not take into account the ability of an SN with a failed sensor to contribute to the functionality of the WSN in practice as a *relay*. Consequently, the size of the resulting paths set is drastically reduced which in turn reduces the value of $R(S)$. It should be explained that the difference between both models in $R(S)$ value for a given deployment is primarily dependent on the number of the tolerable combinations of SNs in the *relay* mode. This is because the higher the number of these combinations, the higher the number of SNs with redundant coverage. Since this coverage redundancy is not accounted for in calculating $R(S)$ using the two-mode SN model, the difference in $R(S)$ between



the two models increases with the increase of the level of coverage redundancy. For example, the deployment S2-D5 has a higher level of coverage redundancy than S5-D5. This is reflected in their difference in $R(S)$ value between the two models, which is 5.4% for the former and 3.9% for the latter.

In order to examine the sensitivity of $R(S)$ of a given deployment to changes in the probabilities of failure of its constituent SNs, we arbitrarily choose one of the deployments in Table 4, deployment S3-D1, and assume all of its 21 SNs are of type 1 only. For this new deployment, we evaluate the reliability at different probabilities of failure ranging from 0.001 to 0.01 for each of the four SN components, assuming the remaining components have the default probabilities of failure given in Table 3. The results obtained are shown in Fig. 7. As expected, the highest value of $R(S)$ is obtained when the probabilities of failure of the four SN components are at their minimum value. Figure 7 also shows that $R(S)$ is less sensitive to changes in the sensor probability of failure than to changes in the other three components probabilities of failure. This can be attributed to the adopted three-mode SN model, for which the SN can contribute to the network functionality in both the *on* and *relay* modes. In the *relay* mode, the SN sensor is not functional. However, for both modes, the SN battery, processor, and transceiver must be functioning. Hence, the reliability of a given deployment is less affected by the change in the sensor probability of failure compared to that of the other components.

7 Conclusions

In this paper, we derived a novel comprehensive reliability metric for heterogeneous WSN deployments of an arbitrary deployment configuration using a combinatorial

approach. In deriving the proposed metric, SNs are modeled as three-mode systems that are characterized by four different probabilities of component failure for the sensor, transceiver, processor, and battery. We addressed the computational problem associated with calculating the reliability of deployments at practical scales using the proposed reliability metric by developing a search algorithm that generates the complete set of paths for a given deployment in a time efficient manner. We applied the proposed metric and search algorithm to several deployments of a case-study surveillance WSN under different operational parameters. Results show that the reliability of a given deployment is mainly a function of its level of SN redundancy and probabilities of failure of its constituent SNs' components. Results also demonstrated the computational efficiency of the developed search algorithm. Moreover, the significance of adopting the proposed three-mode SN model on the evaluated value of WSN reliability as opposed to the conventional simplistic two-mode SN model adopted in existing studies can be observed in the results.

Acknowledgements

The authors extend their appreciation to the anonymous reviewers for their helpful and supportive comments towards improving this paper.

Funding

This open-access publication of this paper is supported by a research grant provided by the American University in Cairo, under grant number 10300000-04131100002-8500-68,665,000.

Authors' contributions

DD and YG conceived the idea and wrote the paper. DD performed the experiments and analyzed the data. YG gave valuable suggestions on the structuring of the paper and assisted in the revising and proofreading. Both authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

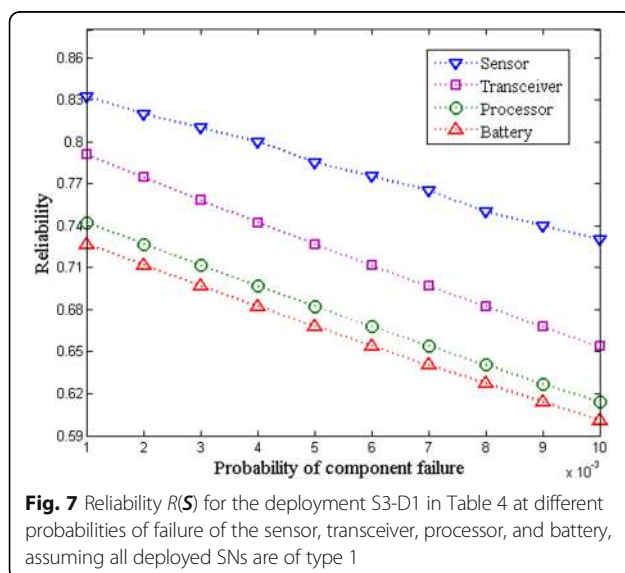
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 24 January 2017 Accepted: 31 July 2017

Published online: 29 August 2017

References

1. A Flammini, E Sisinni, Wireless sensor networking in the Internet of things and cloud computing era, in Proceedings of European Conf. on Solid-State Transducers (EUROSENSOR 2014), Italy, 2014
2. L. Lei, Y. Kuang, X. Shen, K. Yang, J. Qiao, Z. Zhong, Optimal reliability in energy harvesting industrial wireless sensor networks. *IEEE Trans. on Wireless Comm.* **15**, 5399–5413 (2016). doi:10.1109/TWC.2016.2558146
3. W Kuo, MJ Zuo, *Optimal reliability modeling: principles and applications*, 1st edn. (John Wiley, Hoboken, 2003), pp. 85–102
4. C. Zhu, C. Zheng, L. Shu, G. Han, A survey on coverage and connectivity issues in wireless sensor networks. *Network and Computer Appl.* **35**, 619–632 (2012)
5. J Virkki, Y Zhu, Y Meng and L Chen, Reliability of WSN hardware, *Int. J. of Embedded Sys.* **1** (2012). doi:10.5121/ijesa.2011.1201
6. F Koushanfar, M Potkonjak, A Sangiovanni-Vecentelli, Fault-tolerance in wireless sensor networks, in handbook of sensor networks, 1st edn., ed. by M Ilyas, E Mahgoub (CRC Press, Boca Raton, 2005)



7. N Baccour, A Koubaa, L Mottola, MA Zuniga, H Youssef, CA Boano and A Alves, Radio link quality estimation in wireless sensor networks: a survey, *ACM Trans. on Sensor Networks* 8 (2012). doi:10.1145/2240116.2240123
8. MA. Mahmood, K.G. Winston, I. Welch, Reliability in wireless sensor networks: a survey and challenges ahead. *Comput. Netw.* 79, 166–187 (2015)
9. H. AboElFotouh, S. Iyengar, K. Chakrabarty, Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures. *IEEE Trans. Reliab.* 54(145–155) (2005)
10. Y Jin, H Lin, Z Zhang and X Zhang, Estimating the reliability and lifetime of wireless sensor network, in *Proceedings of Int. Conf. on Wireless Communications, Networking and Mobile Computing (WICOM)*, China, 2008
11. A. Damaso, N. Rosa, P. Maciel, Reliability of wireless sensor networks. *MPDI Sensors* 14, 760–785 (2014)
12. X Zhu, Y Lu, J Han and L. Shi, Transmission reliability evaluation for wireless sensor networks, *Hindawi J. Of Distributed Sensor Networks* 10 (2016)
13. Q. Liu, H. Zhang, Weighted voting system with unreliable links. *IEEE Trans. Reliab.* 66(2), 339–350 (2017)
14. C Jaggle, J Neidig, T Grosch and F Dressler, Introduction to model-based reliability evaluation of wireless sensor networks, in *Proceedings of Int. Federation of Automatic Control (IFAC) Workshop on Dependable Control of Discrete Systems*, Italy, 2009
15. I Silva, R Leandro, D Macedo and LA Guedes, A dependability evaluation tool for the Internet of things', *Computers & Electrical Eng.* 39, 806–838 (2013)
16. El Gokce, AK Shrivastava and Y ding, fault tolerance analysis of surveillance sensor systems, *IEEE Trans. on Reliab.* 62, 478–489 (2013)
17. I. Silva, LA. Guedes, P. Portugal, F. Vasques, Reliability and availability evaluation of wireless sensor networks for industrial applications. *MPDI Sensors* 12, 806–838 (2012)
18. H Van-Trinh, N Julien and P Berruet, On-line self-diagnosis based on power measurement for a wireless sensor node, in *Proceedings of the IEEE Workshop on Highly-Reliable Power-Efficient Embedded Designs*, China, 2013
19. A.E. Zonouz, L. Xing, V.M. Vokkarane, Y. Sun, in *Proceedings of Annual Reliability and Maintainability Symposium (RAMS)*. A time-dependent link failure model for wireless sensor networks (2014)
20. Y. Shpungin, Combinatorial approach to reliability evaluation of network with unreliable nodes and unreliable edges. *Int. J. Comput. Sci.* 1(177–183) (2006)
21. IB Gertsbakh and Y Shpungin, Y, *Models of network reliability: analysis, combinatorics, and Monte Carlo*, 1st edn. (CRC Press, Boca Raton, 2010), pp. 17–23
22. M Healy, T Newen and E Lewis, Wireless sensor node hardware: a review, *IEEE Sensors*, 621–624 (2008) doi:10.1109/ICSENS.2008.4716517
23. H Liu, A Nayak and I Stojmenovic, Fault tolerant algorithms/protocols in wireless sensor networks, in *Guide to wireless sensor networks*, ed. by SC Misra, I Woungang, S Misra (Springer-Verlag, Berlin, Germany, 2009), pp. 261–292
24. D. Deif, Y. Gadallah, *Wireless sensor network deployment using a variable-length genetic algorithm* (Proceedings of the Wireless Communications and Networking Conference (WCNC), Turkey, 2014)

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com
