Quantifying the Effects of Homogeneous Interference on Coverage Quality in Wireless Sensor Networks

Qingmiao Liu[1], Qiang Liu[2], Minhuan Wang[3]
School of Management Science and Engineering, Shandong University of Finance and Economics, Jinan, China[1, 2]
Tongji University, Shanghai, China[3]

Abstract—This study develops a coverage perception interference model for Wireless Sensor Networks, focusing on the challenges of homogeneous interference within Regions of Interest. Traditional perception models often overlook areas that, while covered, do not meet the required coverage standards for accurate classification. This model addresses both uncovered areas and those inadequately covered, which are susceptible to classification errors. A propositional space for the coverage model is defined to assess the impact of homogeneous interference on sensor nodes, with the aim of quantifying its effects on network coverage quality and stability in complex environments. The study emphasizes the generation of Basic Probability Assignments using Dempster-Shafer theory, a robust framework for managing uncertain information in sensory data. Probability Density Functions derived from historical and real-time data are utilized to facilitate precise BPA calculations by integrating over specific attribute ranges, thereby enhancing the accuracy and reliability of target detection. Algorithms are also developed to calculate the interference effect BPA, which are integrated with perception coverage models to improve the assessment and optimization of coverage quality. The research enhances the methodological understanding of managing interference in WSNs and offers practical strategies for improving sensor network operations in environments affected by significant interference, boosting the reliability and effectiveness of critical surveillance and monitoring applications.

Keywords—Wireless sensor networks; homogeneous interference; basic probability assignment; coverage quality; Dempster-Shafer theory

I. INTRODUCTION

In the current global landscape, security and surveillance of sensitive areas such as borders, critical infrastructures, and urban centers are of paramount importance. The increasing complexity and sophistication of threats, ranging from unauthorized human intrusions to vehicular entries and wildlife disturbances, necessitate advanced technological solutions that can operate under diverse environmental conditions and provide real-time, reliable data. Wireless Sensor Networks (WSNs) have emerged as a pivotal technology [1-9] in this domain, offering the potential to revolutionize the way these areas are monitored. However, despite their significant potential, the deployment of WSNs in security applications faces several critical challenges that hinder their effectiveness.

One of the primary challenges is the high rate of false positives, which can lead to unnecessary alarms and subsequently drain the resources and attention of security personnel. False positives are predominantly caused by the inability of traditional WSNs to accurately classify the nature of the intrusion [10-14]. For instance, the motion sensors in a network might be triggered by non-threatening entities such as small animals or environmental factors like wind. Such inaccuracies not only undermine the reliability of security protocols but also reduce the trust in these systems.

Moreover, the effectiveness of WSNs is often limited by their capacity for real-time processing and analysis of sensor data. Security applications require immediate responses to detected threats, and any delay in the processing can result in a failure to prevent an intrusion [15-20]. Additionally, the diverse range of intruders and the subtleties in their characteristics necessitate sophisticated algorithms capable of making nuanced distinctions. Current systems predominantly employ simplistic threshold-based algorithms [21-23], which are not only prone to errors but also lack the ability to learn and adapt from past data, thus failing to improve over time.

Current WSN implementations primarily focus on detecting the presence of an intruder rather than classifying the type of intrusion accurately [24-26]. This is a significant limitation, as different types of intrusions require different responses. For instance, the approach to dealing with a human trespasser might differ substantially from that for a wild animal entering a restricted area. Most existing systems utilize basic motion sensors that trigger alarms when interrupted, regardless of the cause. Such systems are unable to distinguish between false alarms caused by non-threatening entities and genuine security breaches, leading to high rates of false positives. This limitation is further exacerbated by the lack of integration of advanced classification algorithms within the sensor networks. While there are robust individual sensor technologies capable of complex data processing [27-30], their integration into network-wide systems that perform real-time analysis and classification is not adequately addressed in existing research.

The integration of advanced computational models, such as those based on Dempster-Shafer theory [31-35], presents a promising solution to these challenges. The Dempster-Shafer theory of evidence allows for the combination of evidence from different sources to arrive at a degree of belief (represented by a belief function) that can handle uncertainty more effectively than traditional probabilistic methods.

Previous studies on Wireless Sensor Networks have primarily concentrated on basic detection algorithms and simplistic models [36-40] that often fail to account for the complexities introduced by homogeneous interference. These studies typically emphasize threshold-based detection

mechanisms, which are inadequate in environments where interference affects multiple sensor nodes uniformly. As a result, these approaches struggle to maintain accurate coverage, leading to increased false positives and unreliable surveillance outcomes. Furthermore, existing research has largely overlooked the integration of advanced probabilistic models to address the uncertainty and ambiguity in sensor data caused by interference.

Given the shortcomings of previous research, there is a clear and pressing need for further investigation into how homogeneous interference impacts the coverage quality of Wireless Sensor Networks. This paper addresses these critical gaps by evaluating the effectiveness of WSNs under the influence of such interference, particularly focusing on interference that uniformly affects multiple sensors. Our study proposes a novel coverage perception interference model that leverages the Dempster-Shafer theory to enhance the robustness and accuracy of WSNs, enabling them to maintain effective coverage even in challenging conditions. Through detailed analysis and modeling, we explore how homogeneous interference compromises the network's ability to sustain reliable coverage and identify vulnerable zones. By incorporating Basic Probability Assignments within the Dempster-Shafer evidence framework, this research provides a nuanced understanding of interference effects, offering practical solutions to improve network reliability. This contribution not only advances the current body of knowledge in WSNs but also establishes a foundation for future research aimed at developing more resilient and adaptive sensor networks capable of operating effectively in complex, interference-prone environments.

This paper is structured as follows: Section II provides a detailed overview of the recognition framework and the mathematical models used in the study, including the implementation of the Dempster-Shafer theory for handling uncertainties in Wireless Sensor Networks (WSNs). Section III introduces the S-I perimeter coverage algorithm, which accounts for homogeneous interference, and discusses its operational rules and algorithmic steps. In Section IV, the simulation results are presented and analyzed, highlighting the impact of interference on coverage quality and the effectiveness of the proposed algorithm. Finally, Section V concludes the paper by summarizing the key findings and suggesting potential directions for future research in improving WSN coverage reliability under interference conditions.

II. PRELIMINARIES

A. Recognition Framework

Wireless Sensor Networks (WSNs), strategically deployed within designated Regions of Interest (ROIs), play a crucial role in enhancing the security and surveillance across vulnerable and sensitive areas by monitoring unauthorized entries from a variety of entities such as humans, animals, and vehicles. These networks are comprised of a coordinated array of sensor nodes, each designated as S_1 （ i=1,2,3…, ξ . These nodes are meticulously programmed and equipped to classify potential intruders into several distinct categories, such as C_1 , C_2 , C_3,...,C_φ, facilitating a targeted response to different types of security breaches.

Each sensor node within the network is outfitted with cutting-edge technology capable of capturing a wide array of detailed attributes from each detected entity. These include visual identifiers like shape and size, infrared signatures that reveal body heat, variations in ambient temperature, and precise measurements of movement speeds. This rich dataset enables a comprehensive and multifaceted analysis of each intrusion, substantially increasing the accuracy of both detection and subsequent classification processes. Beyond mere physical detection, the nodes are also equipped to sense more subtle indicators such as acoustic signals and electromagnetic properties. This capability is essential for distinguishing between organic and mechanical intruders, effectively differentiating between humans, animals, and vehicles. This nuanced approach to intrusion detection is crucial for deploying appropriate security measures and for minimizing false alarms, which are common in less sophisticated systems.

Through the use of advanced data analytics in this article, the information captured by the sensors is analyzed in real-time. This not only ensures timely detection but also enables the network to categorize each object based on its unique attributes and behavior patterns. The adaptability and responsiveness of these networks to a range of environmental stimuli and potential threats are vital, enhancing the overall security protocol of the area.

In our investigation, we explore scenarios involving three primary types of targets, illustrating a methodology and conceptual framework that are universally applicable to scenarios involving the classification of implicit targets into φ (φ>3) categories. Utilizing Dempster-Shafer (D-S) theory, we establish a discernment framework denoted as $\Theta = \{C_1,C_2,C_3\}$. The power set of Θ, represented as 2^Θ, encompasses 2^Θ = { $\emptyset$, A_1 ={ C_1 }, $A_2=\{C_2\}$,$A_3=\{C_3\}$,$A_4=\{C_1,C_2\}$,$A_5=\{C_1,C_3\}$,$A_6=\{C_2, C_3\}$, $A_7=\{C_1,C_2,C_3\}$}, Each element within 2^Θ, $A_\omega(\omega=1,2\ldots,7)$ forms a subset of Θ, symbolizing a specific proposition. Here the propositions$\{C_1\}$、$\{C_2\}$ or $\{C_3\}$ correspond to the sensor classifying the target into categories$\{C_1\}$、$\{C_2\}$ or $\{C_3\}$, respectively. The propositions $\{C_2,C_3\}$,$\{C_1,C_3\}$, $\{C_1,C_2,C_3\}$ indicate ambiguity in the sensing results, suggesting that the target could potentially belong to the combined categories, whereas $\emptyset$ represents the empty set. These propositions are categorized into two types: 1) singleton propositions, where the corresponding subset contains a single element, such as $\{C_1\}$、$\{C_2\}$ and $\{C_3\}$; and 2) multiple subset propositions, where the subset comprises multiple elements, such as $\{C_1,C_2\}$,$\{C_2,C_3\}$,$\{C_1,C_3\}$ and $\{C_1,C_2,C_3\}$.

When a target enters the sensing range of sensor S_i, the sensor perceives each attribute of the target. Based on these attributes, S_i categorizes the target into one of the defined categories, resulting in a classification that is expressed through a basic probability assignment (BPA). The BPA derived from attribute θ by sensor S_i, denoted as m_θ^i, represents a mapping from 2^Θ to the interval [0,1] and adheres to the following conditions:

$$\begin{cases} m_\theta^i(\emptyset) = 0 \\ \sum_{A\subseteq\Theta} m_\theta^i(A) = 1 \end{cases} \quad (1)$$

The sum of all probability masses assigned across the power set must equal one, ensuring a complete and exhaustive representation of all possible classification outcomes.

The probability of the empty set, ∅, is zero, reflecting the premise that every observation can be attributed to at least one category within the framework.

This structured approach not only enhances the precision of target classification within complex environments but also significantly contributes to the development of robust, scalable sensor networks capable of adapting to diverse surveillance and monitoring challenges.

Within the proposition space Θ, A represents any subset, and , $m_\theta^i(A)$ denotes the mass or credibility allocated to proposition A. For instance, upon detecting the attributes θ of an intruding target, sensor node S_i assigns category probability values as follows: $m_\theta^i(C_1) = p_1$, $m_\theta^i(C_2) = p_2$, $m_\theta^i(C_3) = p_3$, $m_\theta^i(\{C_1, C_2\}) = p_4$, $m_\theta^i(\{C_1, C_3\}) = p_5$, $m_\theta^i(\{C_2, C_3\}) = p_6$, $m_\theta^i(\{C_1, C_2, C_3\}) = p_7$, where the sum of p_1 through p_7 equals 1. Given that the invading target A possesses θ attributes, sensor node S_i can measure θ BPA values. For each attribute i=1,2,...,θ, sensor S_i combines these θ BPA values using a special fusion rule denoted as ⊕, thereby deriving a new BPA value m^i, which represents the final detection outcome of the target by sensor S_i.

$$m^i = m_1^i \oplus m_2^i \oplus m_3^i \oplus \cdots m_\theta^i \quad (2)$$

B. Implicitly Targeted BPA Function Generation

The generation of Basic Probability Assignment (BPA) using the Dempster-Shafer (D-S) theory represents a critical step in applying evidence theory to the accurate characterization and identification of targets within sensor networks. The quality of BPA generation crucially influences the precision of perception results and the accuracy of target classification. Currently, the methodology for generating BPA predominantly relies on classification-based approaches, which can be summarized through the following steps: Derivation of classification criteria from historical data; Collection of attribute data from targets awaiting identification, followed by obtaining initial classification results based on the derived criteria; Transformation of these initial classification results into BPA through specific rules. The initial step, forming classification criteria, is pivotal and broadly categorized into three approaches: Expert Systems and Rule-Based Reasoning; Statistical analysis; Machine learning. While each approach offers distinct advantages, they also present challenges such as the maintenance of rule systems, complexity in parameter setting for fuzzy logic, reliance on prior knowledge in Bayesian inference, and the high cost of data annotation in supervised learning. The chosen approach in this research involves using PDFs to fit the attribute values of category targets, subsequently using these fits to generate BPAs for unclassified targets. This method leverages the Gaussian distribution of attribute values to reflect individual variability and measurement errors.

A novel method for determining BPA has been proposed, involving the division of a dataset into a training and a test set. Gaussian models for p attributes are established using the training set and then tested using the test set to determine similarities. Attribute weights are adjusted based on the overlap degree among categories to fine-tune the similarity scores and finalize the BPA, as depicted in the methodology section. This approach provides a structured, objective classification by assessing and integrating new information dynamically, which is essential for robust decision-making in sensor networks.

C. Attribute Modeling Approach

In the discernment framework $\Theta=\{C_1, C_2, C_3 \cdots C_n\}$, each category φ_i (i=1,2,3 $\cdots \tau$ ） is associated with a Gaussian distribution and is characterized by p_j(j=1,2,3…P） attributes. For each category φ_i, the mean and standard deviation for each attribute are derived from the training samples as follows:

The mean value for attribute p, represented as $\bar{X}_p$ is calculated using the formula:

$$\bar{X}_p = \frac{1}{N}\sum_{\tau=1}^{N} x_{\tau,p} \quad (p = 1,2,3 \cdots P) \quad (3)$$

where, $x_{\tau,p}$ is the value of attribute p for the τ-th sample in category φ_i.

The standard deviation for attribute p, denoted as σ_p, is determined by:

$$\sigma_p = \sqrt{\frac{1}{N-1}\sum_{\tau=1}^{N}(x_{\tau,p} - \bar{X}_{\tau,p})^2} \quad (p = 1,2,3 \cdots P) \quad (4)$$

These statistical measures establish the parameters for the Gaussian distribution model of each attribute, which is defined as:

$$\mu_\alpha(x) = e^{-\frac{(x-\bar{X}_p)^2}{2\sigma_p^2}} \quad (5)$$

In this model, the Gaussian-type attribute model is considered a singleton proposition where both $\mu_\alpha(x)$ and $\mu_\beta(x)$ represent individual propositions within the framework. Complex or composite subset propositions are formed by the overlapping regions of these Gaussian membership functions. For example, the composite subset proposition $\{\alpha\beta\}$ is defined by:

$$\mu_{\alpha\beta}(x) = \min\{\mu_\alpha(x), \mu_\beta(x)\} \quad (6)$$

This expression effectively captures the lowest membership value between the two propositions, representing the degree of certainty that the value x belongs to both categories α and β simultaneously. This formulation allows for a nuanced understanding of the intersections and relationships between different category attributes in a multi-dimensional attribute space, facilitating a more precise and sophisticated approach to category classification in statistical analysis and machine learning applications.

D. Similarity Measurement

In the realm of multi-category classification, the construction of attribute weights plays a pivotal role in achieving unbiased results through a comprehensive evaluation of each attribute. The efficacy of an attribute in distinguishing between categories is inversely proportional to the degree of similarity

among the categories it connects. Specifically, if a given attribute exhibits substantial overlap across multiple category models, its discriminatory power is diminished, increasing the likelihood of misclassification and reducing its reliability. Consequently, the Basic Probability Assignment (BPA) generated from such attributes contributes minimally in a multi-category classification setting.

Conversely, attributes that demonstrate low similarity among categories possess enhanced discriminatory capability, thereby affirming their reliability and increasing their contribution to the BPA in the classification process. It becomes imperative to amplify the role of attributes with substantial contributions while diminishing the influence of those with minimal impacts, to foster more objective classification outcomes.

This section introduces and discusses the concept of attribute weighting, where each attribute's weight is inversely related to its degree of overlap among categories, reflecting its discriminative strength and reliability. Suppose μ_{ij} (i=1,2,…,k;j=1,2,…,l) represents the membership function for the j-th attribute of the i-th category, and $\mu_{hj}^{\triangle}$(h=1,2,…,$\frac{k^2-k}{2}$;j=1,2,…,l) denotes the generalized triangular fuzzy number model for the composite subset proposition {AB} for the j-th attribute in the h-th composite category. Let S(x) symbolize the integral or total sum over the defined range of the membership function. The weight ω_j (j=1,2,…,k) for the j-th attribute can be formulated as:

$$\omega_j = 1 - \frac{\sum_{h=1}^{\frac{k^2-k}{2}} S(\mu_{hj}^{\triangle})}{\sum_{i=1}^{k} S(\mu_{ij}) - \sum_{h=1}^{\frac{k^2-k}{2}} S(\mu_{hj}^{\triangle})} \quad (7)$$

Here, a higher value of ω_j (j=1,2,…,k) indicates greater overlap and similarity, thereby assigning a lower weight to the attribute. This weighting approach ensures that attributes contributing significantly to the classification accuracy are emphasized, while those with lesser discriminative power are de-emphasized, optimizing the classification framework for better performance and reliability. This strategy is crucial for enhancing model accuracy and robustness in complex classification landscapes, where the correct identification of category boundaries is vital for effective decision-making and analysis.

In the domain of sensor-based classification, establishing robust Basic Probability Assignments (BPA) for the perception of implicit targets requires a systematic application of Gaussian membership functions. This method takes into account the inherent variability and potential measurement inaccuracies associated with each target attribute, adhering closely to statistical norms found in Gaussian distributions.

For a practical application, consider a category, such as C_1, which comprises multiple targets each characterized by a series of attributes. The attribute values for these targets are systematically analyzed to formulate a data matrix, with each row representing a target and columns corresponding to attributes. The statistical distribution of each attribute is characterized by calculating the mean and standard deviation from this ensemble of data points, facilitating the modeling of attribute behaviors within the target population.

The Gaussian membership function for each attribute in category C_1 is defined to encapsulate the likelihood of attribute values deviating within three standard deviations from the mean. Mathematically, this is expressed as:

$$\mu_{\theta}^{C_1}(x) = \begin{cases} e^{-\frac{(x-\bar{X}_\theta)^2}{2\sigma_\theta^2}}, for\ x\ within\ [\overline{X_\theta} - 3\sigma_\theta, \overline{X_\theta} + 3\sigma_\theta] \\ 0, outside\ this\ interval \end{cases} \quad (8)$$

This formulation precisely quantifies the fit of a given data point x to the modeled attribute distribution, thereby assessing its categorical alignment effectively. It's crucial for ensuring that the classifications are both precise and reflective of the actual attribute distributions, thus reducing misclassifications.

Similarly, this method extends to other categories, such as C_2 and C_3, where Gaussian membership functions are established for each respective attribute. By analyzing the intersection or overlap of these functions across different categories, one can discern the level of distinctiveness or similarity between categories. Such intersections can range from no overlap, where category functions are distinctly separate, to various degrees of partial overlap, illustrating complex inter-attribute relationships.

In the analysis of Gaussian membership functions for categorical classification, the spatial relationships between the curves can reveal significant insights into the interaction and distinctiveness of category attributes. These relationships can generally be categorized into four distinct scenarios, each representing different levels of overlap and separation among the category-specific functions:

No Intersection: In the first scenario, the Gaussian functions for each category are entirely distinct, with no overlap. This separation indicates clear demarcation between categories, suggesting that each category possesses unique attribute values that are significantly different from the others. This scenario is ideal for classification tasks, as it implies high discriminative power for the attributes in distinguishing between categories.

In an ideal scenario where these Gaussian functions are distinct and do not intersect—as depicted in the hypothetical Fig. 1—selecting a point on each curve allows us to determine the precise probability that a sensor node categorizes a target into C_1,C_2 and C_3 based on a specific value of attribute θ. Such configurations where $\mu_{\theta}^{C_1}(x)$ 、 $\mu_{\theta}^{C_2}(x)$ and $\mu_{\theta}^{C_3}(x)$ are independent, facilitate straightforward predictions with high confidence levels about the category of the detected targets.

Partial Intersection: The second scenario involves two of the Gaussian curves intersecting while the third remains separate. This configuration implies that while two categories share some similarity in attribute distributions, they both remain distinctly different from the third category. Such a setup can be useful in identifying overlapping characteristics between the two intersecting categories and leveraging this information to enhance classification accuracy for more complex scenarios.

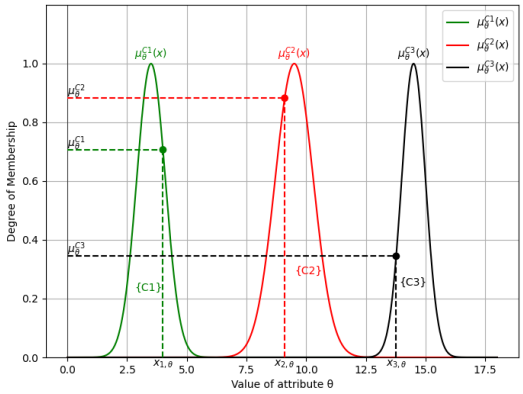

Fig. 1. Scenario of independent gaussian curves.

In contrast, as illustrated in Fig. 2, the Gaussian functions $\mu_\theta^{C_1}(x)$ and $\mu_\theta^{C_2}(x)$ intersect, whereas $\mu_\theta^{C_3}(x)$ remains distinct. The intersection point, noted as $(x_{4,\theta}, \mu_\theta^{C_1,C_2}(x_{4,\theta}))$, marks the area of ambiguity between C_1 and C_2. This area is crucial because it represents the values of θ where the distinction between categories C_1 and C_2 becomes unclear. The upper boundary of this region is defined by the composite subset membership function $\mu_\theta^{C_1,C_2}(x)$, which is the minimum of $\mu_\theta^{C_1,C_2}(x) = min\{\mu_\theta^{C_1}(x), \mu_\theta^{C_2}(x)\}$. This function captures the highest degree of overlap and hence, the maximum uncertainty in classification between these two categories.

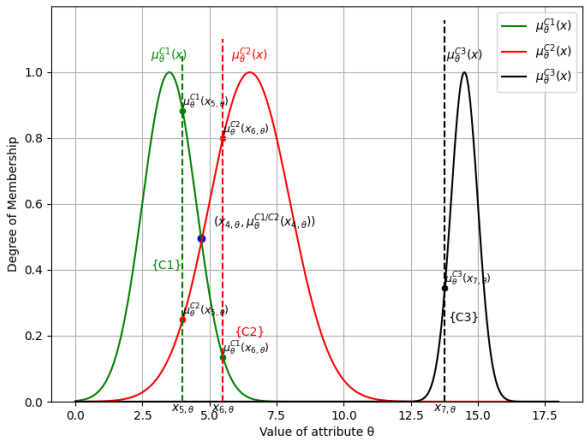

Fig. 2. Two intersecting and one independent GMF curve.

Single Intersection with Others: In the third type, one Gaussian function intersects with each of the other two, but those other two do not intersect with each other. This pattern suggests a central category that shares attributes with the other two categories, which are otherwise distinct from each other. This scenario can be particularly challenging for classification, as it requires careful analysis to ensure accurate category determination.

In Fig. 3, the Gaussian membership functions for the categories C_1,C_2 and C_3 are depicted with specific interactions. The membership functions for C_1 and C_2, $\mu_\theta^{C_1}(x)$ and $\mu_\theta^{C_2}(x)$, intersect at a point defined as $(x_{8,\theta}, \mu_\theta^{C_1,C_2}(x_{8,\theta}))$. Simultaneously, the functions for C_2 and C_3, $\mu_\theta^{C_2}(x)$ and $\mu_\theta^{C_3}(x)$, intersect at $(x_{9,\theta}, \mu_\theta^{C_2,C_3}(x_{9,\theta}))$. The upper limits of these intersections are defined by the composite subset membership functions $\mu_\theta^{C_1,C_2}(x)$ and $\mu_\theta^{C_2,C_3}(x)$, calculated as the minimum values between the respective intersecting functions. This represents a complex but realistic scenario where categories C_1 and C_2 share some common attributes as do categories C_2 and C_3, but C_1 and C_3 remain distinct in this configuration.

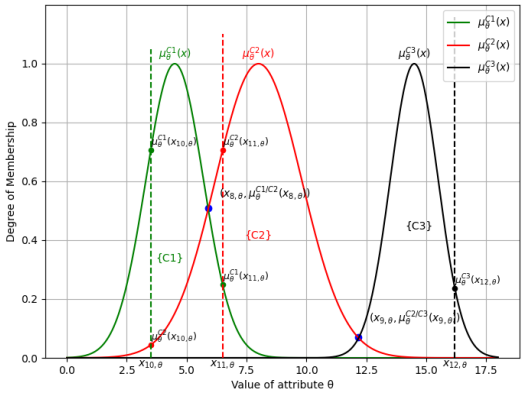

Fig. 3. Two intersecting and separately independent GMF curves.

Mutual Intersection: The final scenario depicts each Gaussian curve intersecting with the other two, indicating a high level of attribute overlap among all three categories. This extensive overlap can lead to higher classification ambiguity and may necessitate more sophisticated analytical techniques or additional data to effectively resolve category assignments.

Fig. 4 illustrates a scenario where all three categories intersect pairwise. The Gaussian curves $\mu_\theta^{C_1}(x)$, $\mu_\theta^{C_2}(x)$ and $\mu_\theta^{C_3}(x)$) each intersect with one another, yielding intersection points at $(x_{13,\theta}, \mu_\theta^{C_1,C_2}(x_{13,\theta}))$、$(x_{14,\theta}, \mu_\theta^{C_2,C_3}(x_{14,\theta}))$ and $(x_{15,\theta}, \mu_\theta^{C_1,C_3}(x_{15,\theta}))$. These points delineate the regions where distinguishing between any two categories becomes challenging due to shared attribute values. The corresponding upper bounds are defined by the composite membership functions $\mu_\theta^{C_1}(x)$,$\mu_\theta^{C_2}(x)$ and $\mu_\theta^{C_3}(x)$), each calculated as the minimum of the intersecting Gaussian functions. This scenario is indicative of a highly intertwined attribute space where each category shares significant overlaps with the others, complicating the classification tasks but also providing rich data for analysis.

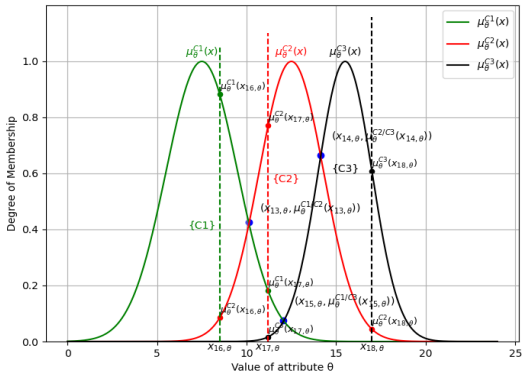

Fig. 4. Pairwise intersecting GMF curves.

E. Interference Effect BPA Generation

In the context of sensor networks, understanding the influence of interference from various sources on sensor nodes is critical, especially how it affects the perception of specific attributes and the subsequent Basic Probability Assignments (BPA) used for decision-making. Interference does not cause sensor failure but introduces biases in the sensors' measurements of attributes, thereby altering the BPA calculations. Here's how to model and calculate the effect of interference on BPA:

Initial BPA Calculation without Interference: First, a sensor S_i measures an attribute θ of a target without any interference. Using the methodology described earlier, the sensor's BPA for the attribute, denoted as m_θ^i, is calculated, representing the sensor's unaltered perception.

BPA Calculation With Interference: The same sensor S_i then measures attribute θ in the presence of a specific interference source G_g. The interference-altered BPA, $m_{\theta,g}^i$, is calculated using the same method as before but adjusted to reflect the combined effect of the original sensor data and the interference. This is done using a specialized operator $\oplus_Z$, where $m_{\theta,g}^i = m_\theta^i \oplus_Z u_{\theta,g}$. This operator blends the original perception effect with the interference effect to produce a new, integrated BPA.

Equation Formulation for Combined BPA: With $m_{\theta,g}^i$ and m_θ^i already derived from the previous steps, the combined BPA equation can be constructed using the operator $\oplus_Z$, finalizing the calculation of the interference-influenced BPA.

Calculating BPA for Other Interference Types: If other interference sources affect sensors designed for different attributes, the above steps (1), (2), and (3) are repeated for each new interference source to calculate its specific impact on BPA.

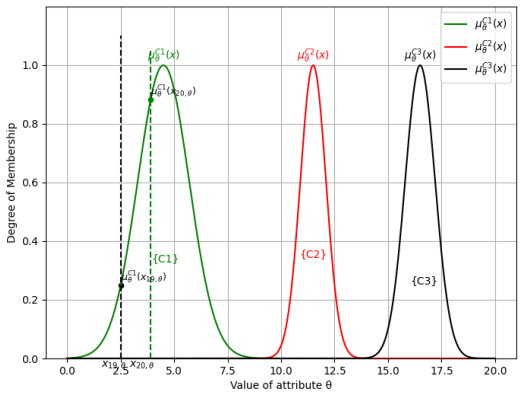

Fig. 5. Membership with interference.

For instance, consider a scenario depicted in a hypothetical Fig. 5, where the original measurement of attribute θ for target 19 is (x_{19}, θ). Under interference, this measurement changes to (x_{20}, θ). Consequently, the BPA generated by the affected sensor node will shift from the original (non-interfered) BPA to a new BPA that is a composite of the original and the interference effects.

In the context of sensor networks, the challenge of accurately interpreting sensor data is compounded when external interference affects the sensor's operation. The concept of Basic Probability Assignment (BPA) is pivotal in quantifying the degree of belief in each possible classification of a target based on sensor data. Consider the scenario where a sensor, without any interference, produces a BPA denoted by mmm. For example, the probabilities that the target belongs to categories C_1, C_2 and C_3 might be given as $m(C_1) = p_1$, $m(C_2) = p_2$, $m(C_3) = p_3$, $m(\{C_1, C_2\}) = p_4$, respectively, with probabilities for combined categories defined similarly.

However, when an interference source affects the sensor, the perception results are altered, introducing deviations in the measured attribute values. The interference effect is itself modeled as a BPA, denoted by g, with its own set of probabilities such as $g(C_1) = p_8$, $g(C_2) = p_9$, $g(C_3) = p_{10}$, $g(\{C_1, C_2\}) = p_{11}$, and so forth, reflecting the impact of the interference on the sensor's ability to classify targets correctly.

The combined effect of the original sensor data and the interference is then calculated using a specialized operator $\oplus_Z$, known as the Dempster combination rule. This rule is employed to integrate the original BPA m and the interference BPA g, resulting in a modified BPA $m^\star$. The probabilities in $m^\star$ are recalculated to reflect this integration, providing new insights into the likely classifications in the presence of interference. For instance, the revised probability that the target belongs to category C_1 in the presence of interference would be updated to $m^\star(C_1) = p_1^\star$, and similarly for the other categories and combinations thereof.

In the context of dealing with sensor interference within wireless networks, the probabilities associated with the Basic Probability Assignment (BPA) for both the non-interfered sensor data and the interference-adjusted data can be methodically calculated using Gaussian membership functions. This calculation treats the probabilities $p_1, p_2, p_3 \cdots\cdots p_7$ associated with the original, undisturbed sensor readings as known quantities. These probabilities reflect the sensor's belief in the target's classification into respective categories without the presence of any distortion.

Similarly, the probabilities $p_1^\star, p_2^\star, p_3^\star \cdots\cdots p_7^\star$ for the interference-affected classifications are derived directly from these Gaussian functions. By applying these well-defined statistical methods, we treat these values as known, calculated based on the sensor's data under the influence of interference.

For the unknown quantities, specifically the interference effect BPA components $p_8, p_9, p_{10} \cdots\cdots p_{14}$, they are not directly observable but can be computed through an established formula that considers the nature of the interference and its impact on the sensor's perception capabilities, refer to the appendix A for detailed computational procedures. This involves leveraging the relationships defined by the Dempster-Shafer theory of evidence, which provides a systematic approach to combine different pieces of evidence, in this case, the original BPA and the interference-induced alterations.

III. S-I PERIMETER COVERAGE ALGORITHM

A. Operational Rules

Sensor Coverage: If a point on the perimeter of sensor node S_i falls within the sensing range of another sensor node S_j, then that point is considered to be covered by S_j.

Segment Coverage: If an entire segment of S_i's perimeter is covered by other sensor nodes excluding S_i itself, it is classified based on the number of covering nodes. For instance, a segment covered by k other nodes is denoted as a k-segment perimeter coverage.

Interference Coverage: If the entire perimeter of a sensor node S_i is within the coverage radius of an interference source I_j, which is the sum of the radius of I_jj and S_i, it is considered to be under the interference perimeter coverage by I_j.

B. Algorithmic Steps

1. Identify Covered Segments: For each sensor node S_j, calculate the segments of other nearby sensor nodes S_i that fall within a double radius distance (2r). These segments are represented by angular intervals $[\alpha_i, L, \alpha_i, R]$.

2. Construct and Sort Points: For all neighboring nodes within a distance less than 2r from S_i, place the points α_i, L and α_i, R on the circular boundary [0, 2π]. These points are sorted in a list L and marked as either the start or end of a covered segment.

3. Determine Coverage Frequency: Traverse the circular boundary [0, 2π] using the sorted list L, from left to right, to determine the coverage status of S_j and count the number of times each segment is covered by other sensor nodes, denoted as $N_{S_{seg}}$.

4. Check Interference Influence: For each interference source I_j, check if S_j is within the interference coverage. If so, place corresponding points α_i, L and α_i, R on [0, 2π].

5. Calculate Interference Coverage Count: Using the sorted list L, determine the number of times each segment is covered by interference sources, represented as $N_{I_{seg}}$.

MSR defined by the arbitrary segmentation of the perimeter of a sensing node S_i are referred to as the MSRs associated with node S_i. For instance, as depicted in Fig. 6, the specific associations between nodes and MSRs are as follows:

MSR 2 and MSR 3 are associated with S_1; MSR 4 and MSR 5 are associated withS_2; MSR 6 and MSR 7、MSR 8 and MSR 9、 MSR 10 and MSR 11are associated with S_3; MSR 9 and MSR 10、MSR 8 and MSR 11are associated with S_4; MSR 6 and MSR 9、MSR 7 and MSR 8、MSR 12 and MSR 13 are associated with S_5; MSR 14 and MSR 15 are associated with S_6; MSR 15 and MSR 16 are associated with S_7; MSR 13 and MSR 14 are associated withS_8.

This structured association allows for a detailed analysis of how each segment of a sensing node's perimeter interacts with the coverage provided by other nodes, facilitating the calculation of coverage frequencies and the influence of interference sources on the network's overall sensing reliability.

MSR1 and MSR2 are within the sensing range ofS_1, MSR2, MSR3, MSR4, MSR21, and MSR22 are within the sensing range of S_2, and MSR4, MSR5, MSR6, MSR9, MSR10, MSR19, MSR20, MSR21, MSR23, and MSR26 fall within the sensing range of S_3. MSR6, MSR7, MSR8, MSR9, MSR25, and MSR26 are covered by S_4, while MSR8, MSR9, MSR10, MSR11, MSR12, MSR18, and MSR19 are within the sensing range of S_5. Similarly, MSRs covered by S_6 to S_{10} can be determined based on their sensing ranges.

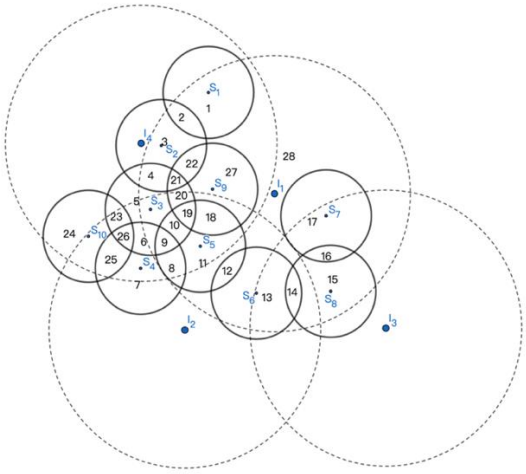

Fig. 6. Perimeter coverage considering homogeneous interference.

The number of times an MSR MSR_p is covered by other sensing nodes is denoted as Q_s, which can be calculated using the function MSR_p $(N_{S_{seg}})$. Similarly, the number of times MSR_q is covered by interference nodes is denoted as G_i, which can be calculated using the function MSR_q $(N_{I_{seg}})$. The function details are as Appendix B.

C. Model Example

After obtaining the sensing coverage count Q_s and the interference coverage count G_i through these functions, the confidence level of the corresponding MSR can be calculated. If a target T_1 enters MSR r, the BPA of the sensing result for T_1 by the sensing node is m, and the interference effect BPA by the interference source is g. Considering the interference effect, the final sensing result in MSR r for the target T_1 is $M_i = (\oplus m)^{Q_s} \oplus (\oplus g)^{G_i}$, where $(\oplus m)^{Q_s}$ represents the combination of Q_s BPAs, such as $(\oplus m)^5$= m ⊕ m⊕ m⊕ m⊕ m. The belief degree bel(MSR_i) of MSR r can then be obtained. According to the reliability metric formula $D^{\delta}_{C_\xi}$, we can compute $D^{\delta}_{C_1}$、$D^{\delta}_{C_2}$、$D^{\delta}_{C_3}$、$D^{\delta}_{\{C_1,C_2\}}$、$D^{\delta}_{\{C_1,C_3\}}$、$D^{\delta}_{\{C_2,C_3\}}$ and $D^{\delta}_{\{C_1,C_2,C_3\}}$.

Based on this analysis, an algorithm to evaluate the reliability of WSN coverage considering the interference is proposed:

For any MSR in the ROI:

Consider the final sensing result $M_i = (\oplus m)^{Q_s} \oplus (\oplus g)^{G_i}$

Compute $D^{\delta}_{C_1}$、 $D^{\delta}_{C_2}$、 $D^{\delta}_{C_3}$、 $D^{\delta}_{\{C_1,C_2\}}$、 $D^{\delta}_{\{C_1,C_3\}}$、 $D^{\delta}_{\{C_2,C_3\}}$ and $D^{\delta}_{\{C_1,C_2,C_3\}}$

To further illustrate the process of this algorithm, we take the sensing node S_3 in Fig. 6 as an example. Besides being perimeter-covered by other sensing nodes S_2、 S_4、 S_5、 S_9, and S_{10}, node S_3 is also influenced by interference sources I_1、 I_2, and I_4. The coverage of various segments of node S_3's perimeter by other sensing nodes is illustrated in Fig. 7.

In a detailed examination of the sensing perimeter associated with sensor node S_3, we observe that interference sources I_1、 I_2, and I_4 impact its operational efficacy. As demonstrated in Fig. 7, the sequence list provides insights into the perimeter segments of S_3 that are influenced by these interference sources. Table I (refer to Appendix C) summarizes the count of coverage occurrences for each segment of S_3's perimeter, reflecting the interplay between sensory and interference coverages.

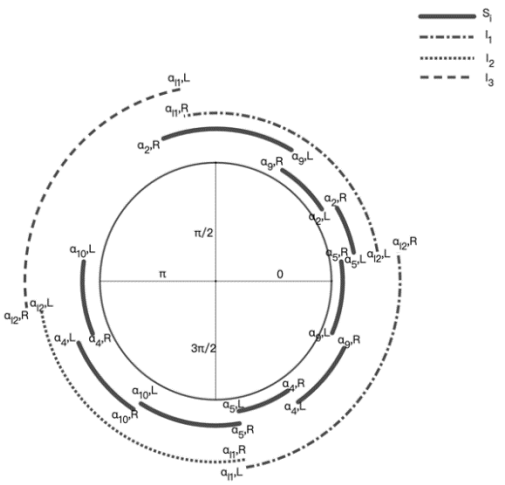

Fig. 7. Perimeter coverage sorted list of S_3.

In the detailed examination of the coverage dynamics within a sensor network, specific attention is directed toward Sensor Node S_3. This node serves as a focal point for evaluating the MSRs related to its periphery, delineated in accordance with the established network protocols and environmental interactions. The process involves a meticulous traversal and assessment of all related MSRs, denoted as MSR_p, to ascertain their sensory coverage status, which is captured in the ensuing coverage information table.

Additionally, the examination extends to the MSRs associated with Sensor Node S_2, including MSR 1 and MSR 2. These regions, lying outside the sensory radius of S_2, experience coverage counts of 1 and 2 respectively, reflecting varying levels of sensor influence. Furthermore, an expansive list of MSRs associated with Sensor Node S_5 includes regions from MSR 5 to MSR 28. Among these, MSR 12, located within S_5's sensory radius, exhibits a coverage count of 2, signifying robust sensor activity, whereas MSR 13, outside this radius, is covered once, indicating lesser sensory influence.

The remaining MSRs, specifically MSR 14 to MSR 17, relate to Sensor Node S_6. MSR 14, found within the sensory radius, is covered twice, affirming its significant sensory engagement. In contrast, MSR 15, outside the sensory radius, demonstrates a reduced coverage count of 1. Similar patterns are observed with MSR 16 related to Sensor Node S_8, covered twice within the sensory radius, and MSR 17, with a coverage count of 1 outside the radius.

Post compilation of sensory coverage counts for all pertinent MSRs, the interference coverage counts, denoted G_i, for these regions are calculated using the function MSR_q. This leads to a nuanced understanding of both the sensory and interference dynamics impacting each MSR.

Upon obtaining the sensory (Q_s) and interference (G_i) coverage counts for the smallest sensing regions, the ultimate sensory results considering interference effects are derived through the formula $M_i = (\bigoplus m)^{Q_s} \bigoplus (\bigoplus g)^{G_i}$. Subsequently, the reliability indices $D^{\delta}_{C_\xi}$ for various configurations are computed, providing a quantitative measure of the network's coverage reliability across diverse environmental and operational scenarios.

IV. Model Simulation

In the ongoing research to enhance the comprehension and reliability of belief coverage in sensory networks, the integration of Monte Carlo simulation offers a robust methodology to analyze the impact of varying parameters on system robustness. This advanced approach not only facilitates a detailed assessment across multiple scenarios but also augments the analytical capabilities concerning sensory and interference node deployments within a defined Region of Interest (ROI).

In Fig. 8, thirteen sensory nodes and four interference nodes are randomly positioned within a 100 by 100 ROI. The sensory range, depicted by blue circles, extends a radius of 10 units, while the interference range, illustrated with red dashed circles, extends a radius of 15 units. Using this setup as a basis, we evaluate the reliability metrics $D^{\delta}_{C_1}$、 $D^{\delta}_{C_2}$、 $D^{\delta}_{C_3}$、 $D^{\delta}_{\{C_1,C_2\}}$、 $D^{\delta}_{\{C_1,C_3\}}$、 $D^{\delta}_{\{C_2,C_3\}}$ and $D^{\delta}_{\{C_1,C_2,C_3\}}$. These assessments employ a Monte Carlo method to explore how various parameters influence system reliability, increasing the resolution of our point matrix to 500 by 500 to enhance simulation accuracy. The Gaussian Membership Functions (GMFs) for categories C_1, C_2, and C_3 are defined with respective means and standard deviations of 7.5 and 2, 12.5 and 2.5, and 15.5 and 2.

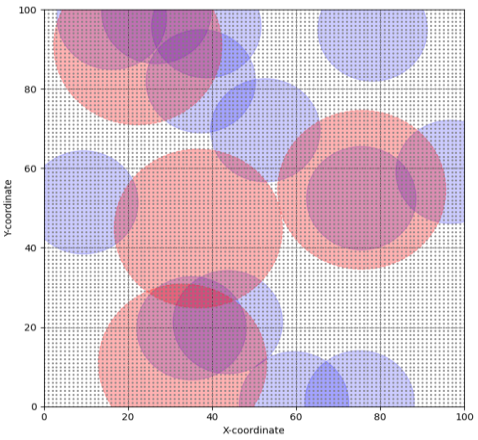

Fig. 8. Random deployment of sensor nodes and interference nodes.

These functions are graphically represented in Fig. 9. Notable intersections of these functions occur at (9.71, 0.54) between $\mu^{C_1}(x)$ and $\mu^{C_2}(x)$, and at (11.48, 0.14) between $\mu^{C_1}(x)$ and $\mu^{C_3}(x)$, and at (14.15, 0.8) between $\mu^2(x)$ and $\mu^3(x)$. Fig. 10 and Fig. 11 illustrate the computed reliability indices. Setting the confidence threshold δ at 0 and the interference factor I at 1, where I=1 implies no consideration of interference effects, the comprehensive ROI coverage rate is 0.9739.

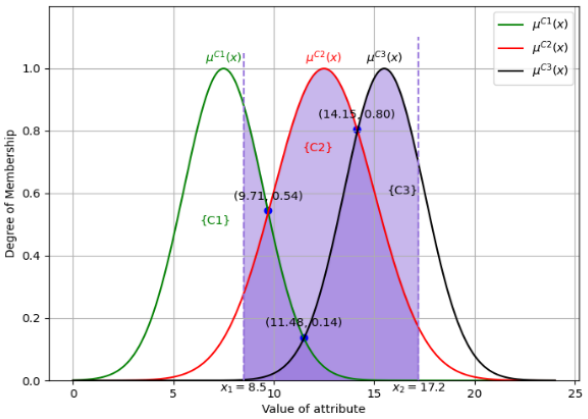

Fig. 9. Gaussian membership function simulation.

Assuming classification is based solely on a single attribute that varies from 8.5 to 17.2, For values of x ranging from 0 to 4.85, $D^0_{C_1}$ dominates at 0.9739, with other classifications scoring zero, indicating that targets within the full sensory coverage are classified exclusively as C_1. At critical values of x such as 9.71 and 14.15, peak values are observed for $D^0_{\{C_1,C_2\}}$ and $D^0_{\{C_2,C_3\}}$, respectively.

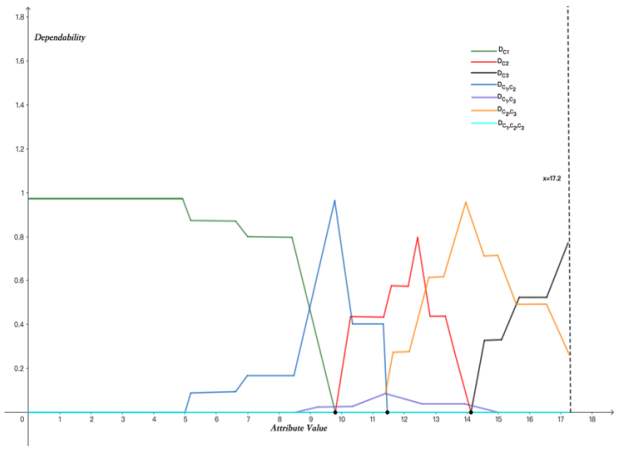

Fig. 10. Reliability trend (**I**=1).

As x increases, the category shifts: from 4.85 to 9.71, the proportion of regions classifying the target as C_1 decreases, while $D^0_{\{C_1,C_2\}}$ grows, indicating ambiguity in classification between C_1 and C_2. Between 9.71 and 12.5, $D^0_{C_2}$ increases directly with x, peaking at x=12.5. Beyond 14.15, more regions start classifying the target as C_3, although some areas remain uncertain between C_2 and C_3, until a definitive classification as C_3 becomes predominant as x approaches 17.2.

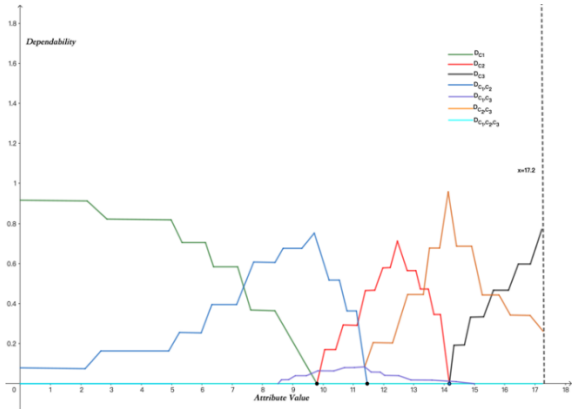

Fig. 11. Reliability trend (**I**=0.7).

In Fig. 11, with δ set at 0 and I at 0.7, significant shifts occur in the reliability metrics compared to when I=1, underscoring how interference significantly impacts sensory coverage reliability. Despite these variations, the overall coverage rate remains 0.9739, affirming robust system performance under varied conditions. As x ranges from 0 to 7.25, most of the ROI classifies targets as C_1; between 11.48 and 12.67, C_2 becomes more likely; and from 15.53 to 17.2, the classification increasingly favors C_3.

Setting the confidence threshold δ to zero allows for a more detailed observation of the reliability metrics for different classifications: $D^\delta_{C_1}$、$D^\delta_{C_2}$、$D^\delta_{C_3}$、$D^\delta_{\{C_1,C_2\}}$、$D^\delta_{\{C_1,C_3\}}$、$D^\delta_{\{C_2,C_3\}}$ and $D^\delta_{\{C_1,C_2,C_3\}}$, with attribute values ranging from 0 to 17.2 and interference factors between 0.7 and 1. The overall trends for these functions are illustrated in Fig. 12 to Fig. 17.

In Fig. 12, within the attribute value range of 9.71 to 17.2, changes in the interference factor do not affect the reliability outcome $D^\delta_{C_1}$. However, for values from 0 to 9.71, as the interference factor decreases, the reliability for category C_1 similarly declines, and the lower the interference factor, the greater the reduction in reliability, indicating that the disruptive effects of interference sources are particularly significant within specific attribute value ranges.

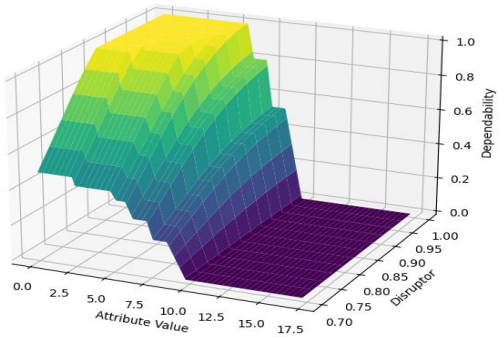

Fig. 12. Overall trend of the function $D^\delta_{C_1}$.

This figure clearly demonstrates the relationship between external intrusion attribute values and the reliability of the sensing coverage system. Across the higher attribute value range of 9.71 to 17.2, regardless of changes in the interference factor,

the system's sensing classification reliability remains stable, indicating that the sensor network's monitoring of attribute values has become stable and robust. When attribute values fall below 9.71, the reliability of the coverage system significantly decreases with increasing interference factor; thus, when designing sensing coverage systems, particular attention needs to be paid to the effects of interference in scenarios with low attribute values, as smaller interference factors mean greater disruption from external interference sources, leading to faster declines in system reliability. This may be due to the low intensity of the target's relevant attributes under these conditions, making them more susceptible to environmental noise and electromagnetic interference, thus reducing the sensing nodes' detection accuracy.

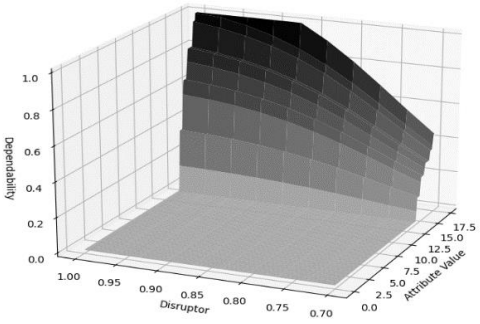

Fig. 13. Overall trend of the function $\boldsymbol{D^{\delta}_{C_2}}$.

In Fig. 13, for attribute values within the ranges of 0 to 9.71 and 14.15 to 17.2, there are no MSRs that classify the sensing results as category C_2, indicating that the attribute values of the intrusion targets are either too low to elicit an adequate system response or too high, exceeding the optimal operational range of the sensing coverage system. From 9.71 to 14.15, the reliability results of sensing classification for $D^{\delta}_{C_2}$ initially increase and then decrease, particularly as the attribute value reaches 12.5, where the characteristics of the intrusion target highly align with the features of category C_2, resulting in maximum reliability for this classification—a peak symbolizing the sensing coverage system's highest confidence level in assigning targets to category C_2. Thereafter, the degree of membership for classifying targets as C_2 gradually diminishes until it reaches zero, with the interference factor I and the reliability of classification $D^{\delta}_{C_2}$ being directly correlated—the larger the interference factor, the higher the classification reliability.

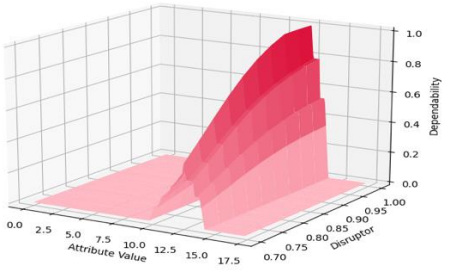

Fig. 14. Overall trend of the function $\boldsymbol{D^{\delta}_{C_3}}$.

In Fig. 14, within the range of 0 to 14.15, the reliability outcome of sensing classification $D^{\delta}_{C_3}$ does not fluctuate with changes in the interference factor, but from 14.15 to 17.2, the degree of membership for classifying targets as C_3, $D^{\delta}_{C_3}$, steadily increases with rising attribute values. Similarly, $D^{\delta}_{C_3}$ shows a positive correlation with the interference factor I, with an increase in the factor enhancing the classification result's reliability, which, in turn, results in a decrease in $D^{\delta}_{\{C_2,C_3\}}$ as shown in Fig. 17.

Fig. 15 illustrates that from 0 to 8.5, the changes in $D^{\delta}_{C_1}$ and $D^{\delta}_{\{C_1,C_2\}}$ display a symmetrical trend due to the intensified effect of interference, causing uncertainty in the sensing classification results right from the start ($D^{\delta}_{\{C_1,C_2\}} \neq 0$). From 8.5 to 9.71, the number of MSRs unable to determine the category of the intrusion target gradually increases, and from 9.71 to 11.48, the reliability of classification results $D^{\delta}_{\{C_1,C_2\}}$ consistently decreases, due to the attribute values increasing the affiliation of the intrusion targets to category C_2more frequently.

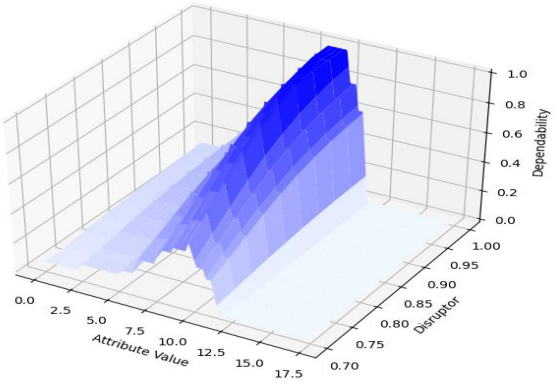

Fig. 15. Overall trend of the function $\boldsymbol{D^{\delta}_{\{C_1,C_2\}}}$.

Fig. 16 indicates that within the range of 8.5 to 15, there are portions of the sensing coverage area unable to correctly classify intrusion targets as either C_1 or C_3, reaching a peak number of problematic MSRs at 11.48, although this has limited impact on the overall reliability of classification results, indirectly showing that these parts of the sensing coverage due to negative effects from interference sources have insufficient detection accuracy.

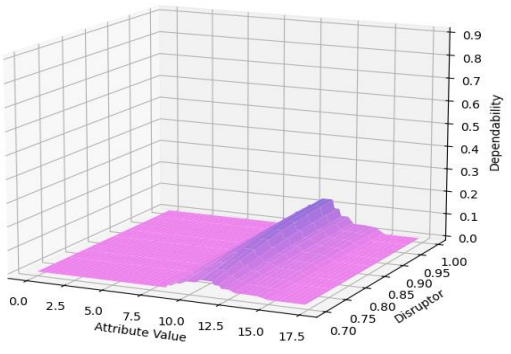

Fig. 16. Overall trend of the function $\boldsymbol{D^{\delta}_{\{C_1,C_3\}}}$.

Fig. 17 shows that the interference factor impacts the reliability of sensing coverage $D^{\delta}_{\{C_2,C_3\}}$ only within the specific attribute value range of 11.48 to 17.2, not significantly in all cases, allowing for an assessment of the dynamic nature and sensitivity of the sensing coverage system to external condition changes. From 11.48 to 14.15, as the interference factor increases, the reliability of coverage $D^{\delta}_{\{C_2,C_3\}}$ also gradually improves, with the number of MSRs unable to correctly classify targets within the ROI incrementally increasing. From 14.15 to 17.2, the weaker the interference effect, the stronger the reliability of sensing coverage $D^{\delta}_{\{C_2,C_3\}}$.

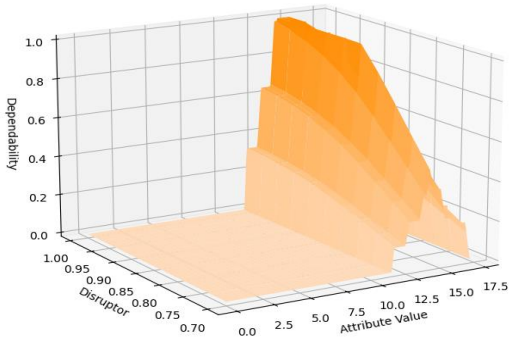

Fig. 17. Overall trend of the function $D^{\delta}_{\{C_2,C_3\}}$.

V. Conclusion

The research presented in this study contributes a novel and robust approach to enhancing the security and reliability of Wireless Sensor Networks (WSNs) by addressing the critical issue of false positives and improving intruder classification accuracy. The use of Dempster-Shafer theory for evidence combination is a key innovation, offering a powerful means to manage the uncertainty inherent in sensor data, particularly in environments where interference and overlapping signals are prevalent. This methodology stands out for its ability to integrate multiple sources of evidence, thereby refining the overall decision-making process and enhancing the reliability of intrusion detection systems.

Despite these strengths, there are several areas where the model could be further refined and extended. One significant limitation of the current approach is its static nature. While the model effectively reduces false positives by distinguishing between different types of intruders, it does so based on predefined Gaussian membership functions and belief structures that may not adapt well to rapidly changing conditions. In dynamic environments, where the nature of threats can evolve quickly, this rigidity could lead to reduced effectiveness over time. Therefore, integrating machine learning algorithms into the framework could be a promising direction for future research. Such integration would enable the model to learn from real-time data, adapt its parameters dynamically, and improve its accuracy in response to changing environmental factors and threat landscapes.

Moreover, while the model has been demonstrated to work effectively in the context of high-security areas, its application to larger and more complex WSNs raises questions about scalability. As the network size increases, the computational demands associated with processing and integrating data from numerous sensors could become significant. This potential bottleneck suggests a need for optimization techniques that can maintain the model's efficiency in larger deployments. For instance, hierarchical or distributed processing methods could be explored to manage the computational load more effectively, ensuring that the system remains responsive and reliable even as the scale of the network grows.

Another important consideration is the model's applicability beyond the immediate context of high-security monitoring. The principles underlying the proposed framework—such as the use of evidence theory and the focus on managing uncertainty—could be valuable in a range of other domains. For example, in wildlife tracking or traffic management, where sensor networks must operate under varying and often unpredictable conditions, the ability to accurately classify and respond to different types of entities is crucial. Expanding the framework to address these broader applications could provide substantial societal benefits, making WSNs more versatile and effective across diverse fields.

In addition to these technical considerations, it is also worth reflecting on the broader implications of this research in the context of WSN development. The growing reliance on sensor networks in critical infrastructure and security applications means that the robustness and reliability of these systems are of paramount importance. By providing a framework that can better manage the inherent uncertainties and complexities of these environments, this research contributes to the advancement of WSN technology as a whole. However, as with any emerging technology, continuous improvement and adaptation are necessary to keep pace with evolving challenges. Future research should not only focus on technical enhancements but also consider the ethical and societal implications of deploying increasingly autonomous and intelligent sensor networks in sensitive areas.

In conclusion, while the current study represents a significant step forward in the development of more reliable and adaptable WSNs, there is ample room for further exploration and refinement. By addressing the limitations of the current model and expanding its applicability, future work can build on this foundation to create even more effective and versatile sensor networks, capable of meeting the demands of a wide range of modern applications.

Acknowledgment

We extend our deepest gratitude to the Shandong Province Social Science Planning Research Project (Grant No. 23CXWJ04), the National Natural Science Foundation of China (Grant No. 61403230), and the Natural Science Foundation of Shandong Province (Grant No. ZR2020MG011) for their generous support. Their contributions were invaluable in the realization of our research. The insights and outcomes presented in this work are a testament to their commitment to advancing knowledge in our field.

References

[1] MOLKA-DANIELSEN J, ENGELSETH P, OLEšNANíKOVá V, et al. Big data analytics for air quality monitoring at a logistics shipping base via autonomous wireless sensor network technologies; proceedings of the

2017 5th international conference on enterprise systems (ES), F, 2017 [C]. IEEE.

[2] SHAKOOR N, NORTHRUP D, MURRAY S, et al. Big data driven agriculture: big data analytics in plant breeding, genomics, and the use of remote sensing technologies to advance crop productivity [J]. The Plant Phenome Journal, 2019, 2(1): 1-8.

[3] KAUSHIK S. Big Medical Data Analytics Using Sensor Technology [M]. Efficient Data Handling for Massive Internet of Medical Things: Healthcare Data Analytics. Springer. 2021: 45-70.

[4] UDDIN M, SYED-ABDUL S. Data analytics and applications of the wearable sensors in healthcare: an overview [J]. Sensors, 2020, 20(5): 1379.

[5] BLAKE R, MICHALIKOVA K F. Deep learning-based sensing technologies, artificial intelligence-based decision-making algorithms, and big geospatial data analytics in cognitive internet of things [J]. Analysis and Metaphysics, 2021, 20: 159-73.

[6] ALEXAKIS T, PEPPES N, DEMESTICHAS K, et al. A distributed big data analytics architecture for vehicle sensor data [J]. Sensors, 2022, 23(1): 357.

[7] BATOOL S, SAQIB N A, KHATTACK M K, et al. Identification of remote IoT users using sensor data analytics; proceedings of the Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 1, F, 2020 [C]. Springer.

[8] HAILE M A, HAILE D T, ZERIHUN D. Real-time sensor data analytics and visualization in cloud-based systems for forest environment monitoring [J]. International Journal of Advances in Signal and Image Sciences, 2023, 9(1): 29-39.

[9] HARB H, MANSOUR A, NASSER A, et al. A sensor-based data analytics for patient monitoring in connected healthcare applications [J]. IEEE Sensors Journal, 2020, 21(2): 974-84.

[10] LIAO H-J, LIN C-H R, LIN Y-C, et al. Intrusion detection system: A comprehensive review [J]. Journal of Network and Computer Applications, 2013, 36(1): 16-24.

[11] OZKAN-OKAY M, SAMET R, ASLAN Ö, et al. A comprehensive systematic literature review on intrusion detection systems [J]. IEEE Access, 2021, 9: 157727-60.

[12] PANIGRAHI R, BORAH S. A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems [J]. International Journal of Engineering & Technology, 2018, 7(3.24): 479-82.

[13] SHENFIELD A, DAY D, AYESH A. Intelligent intrusion detection systems using artificial neural networks [J]. Ict Express, 2018, 4(2): 95-9.

[14] WU X, HONG D, CHANUSSOT J. Convolutional neural networks for multimodal remote sensing data classification [J]. IEEE Transactions on Geoscience and Remote Sensing, 2021, 60: 1-10.

[15] BUTUN I, MORGERA S D, SANKAR R. A survey of intrusion detection systems in wireless sensor networks [J]. IEEE communications surveys & tutorials, 2013, 16(1): 266-82.

[16] DREWEK-OSSOWICKA A, PIETROŁAJ M, RUMIńSKI J. A survey of neural networks usage for intrusion detection systems [J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(1): 497-514.

[17] KABIR E, HU J, WANG H, et al. A novel statistical technique for intrusion detection systems [J]. Future Generation Computer Systems, 2018, 79: 303-18.

[18] KARATAS G, DEMIR O, SAHINGOZ O K. Deep learning in intrusion detection systems; proceedings of the 2018 international congress on big data, deep learning and fighting cyber terrorism (IBIGDELFT), F, 2018 [C]. IEEE.

[19] KHRAISAT A, GONDAL I, VAMPLEW P, et al. Survey of intrusion detection systems: techniques, datasets and challenges [J]. Cybersecurity, 2019, 2(1): 1-22.

[20] LANSKY J, ALI S, MOHAMMADI M, et al. Deep learning-based intrusion detection systems: a systematic review [J]. IEEE Access, 2021, 9: 101574-99.

[21] KHAN B A, SHARIF M, RAZA M, et al. An approach for surveillance using wireless sensor networks (WSN) [J]. Journal of Information & Communication Technology, 2007, 1(2): 35-42.

[22] MOSTAFAEI H, CHOWDHURY M U, OBAIDAT M S. Border surveillance with WSN systems in a distributed manner [J]. IEEE Systems Journal, 2018, 12(4): 3703-12.

[23] LIAO Y, MOLLINEAUX M, HSU R, et al. Snowfort: An open source wireless sensor network for data analytics in infrastructure and environmental monitoring [J]. IEEE Sensors Journal, 2014, 14(12): 4253-63.

[24] TIDJON L N, FRAPPIER M, MAMMAR A. Intrusion detection systems: A cross-domain overview [J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3639-81.

[25] BHATI N S, KHARI M, GARCíA-DíAZ V, et al. A review on intrusion detection systems and techniques [J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2020, 28(Supp02): 65-91.

[26] CASAS P, MAZEL J, OWEZARSKI P. Unsupervised network intrusion detection systems: Detecting the unknown without knowledge [J]. Computer Communications, 2012, 35(7): 772-83.

[27] LAOUIRA M L, ABDELLI A, OTHMAN J B, et al. An efficient WSN based solution for border surveillance [J]. IEEE Transactions on Sustainable Computing, 2019, 6(1): 54-65.

[28] AL GHAMDI A, ASEERI M, AHMED M R. A novel trust and reputation model based WSN technology to secure border surveillance [J]. International Journal of Future Computer and Communication, 2013, 2(3): 263.

[29] SERT S A, ONUR E, YAZICI A. Security attacks and countermeasures in surveillance wireless sensor networks; proceedings of the 2015 9th International Conference on Application of Information and Communication Technologies (AICT), F, 2015 [C]. IEEE.

[30] VIANI F, OLIVERI G, DONELLI M, et al. WSN-based solutions for security and surveillance; proceedings of the The 40th European Microwave Conference, F, 2010 [C]. IEEE.

[31] YAGER R R, KACPRZYK J, FEDRIZZI M. Advances in the Dempster-Shafer theory of evidence [M]. John Wiley & Sons, Inc., 1994.

[32] YANG B-S, KIM K J. Application of Dempster–Shafer theory in fault diagnosis of induction motors using vibration and current signals [J]. Mechanical Systems and Signal Processing, 2006, 20(2): 403-20.

[33] DENOEUX T. A neural network classifier based on Dempster-Shafer theory [J]. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2000, 30(2): 131-50.

[34] ZADEH L A. A simple view of the Dempster-Shafer theory of evidence and its implication for the rule of combination [J]. AI magazine, 1986, 7(2): 85-.

[35] KLIR G J, RAMER A. Uncertainty in the Dempster-Shafer theory: a critical re-examination [J]. International Journal of General System, 1990, 18(2): 155-66.

[36] BENELHOURI A, IDRISSI-SABA H, ANTARI J. An evolutionary routing protocol for load balancing and QoS enhancement in IoT enabled heterogeneous WSNs [J]. Simulation Modelling Practice and Theory, 2023, 124: 102729.

[37] HOSSEINZADEH M, YOO J, ALI S, et al. A cluster-based trusted routing method using fire hawk optimizer (FHO) in wireless sensor networks (WSNs) [J]. Scientific Reports, 2023, 13(1): 13046.

[38] JARADAT Y, MASOUD M, JANNOUD I, et al. Analysis of the optimal number of clusters and probability in homogeneous unreliable WSNs [J]. Multimedia Tools and Applications, 2023, 82(25): 39633-52.

[39] LOHAR L, AGRAWAL N K, GUPTA P, et al. A novel approach based on bio - inspired efficient clustering algorithm for large - scale heterogeneous wireless sensor networks [J]. International Journal of Communication Systems, 2023, 36(8): e5472.

[40] WANG N, ZHANG S, ZHANG Z, et al. Lightweight and Secure Data Transmission Scheme Against Malicious Nodes in Heterogeneous Wireless Sensor Networks [J]. IEEE Transactions on Information Forensics and Security, 2023.

APPENDIX A

$$K=m(C_1)\,g(C_2)+m(C_1)\,g(C_3)+m(C_1)\,g(\{C_2,C_3\})+m(C_2)\,g(C_1)+m(C_2)\,g(C_3)+m(C_2)\,g(\{C_1,C_3\})+m(C_3)\,g(C_1)+m(C_3)\,g(C_2)+m(C_3)\,g(\{C_1,C_2\})=p_1p_9+p_1p_{10}+p_1p_{13}+p_2p_8+p_2p_{10}+p_2p_{12}+p_3p_8+p_3p_9+p_3p_{11}$$

$$p_1^{\star}=m^{\star}(C_1)=\frac{1}{1-K}[m(C_1)\,g(C_1)+m(C_1)\,g(\{C_1,C_2\})+m(C_1)\,g(\{C_1,C_3\})+m(C_1)\,g(\{C_1,C_2,C_3\})+\ m(\{C_1,C_2\})g(C_1)+\ m(\{C_1,C_3\})g(C_1)+m(\{C_1,C_2,C_3\})g(C_1)]=\frac{1}{1-K}(p_1p_8+p_1p_{11}+p_1p_{12}+p_1p_{14}+p_4p_8+p_5p_8+p_7p_8)$$

$$p_2^{\star}=m^{\star}(C_2)=\frac{1}{1-K}[m(C_2)\,g(C_2)+m(C_2)\,g(\{C_1,C_2\})+m(C_2)\,g(\{C_2,C_3\})+m(C_2)\,g(\{C_1,C_2,C_3\})+\ m(\{C_1,C_2\})g(C_2)+\ m(\{C_2,C_3\})g(C_2)+m(\{C_1,C_2,C_3\})g(C_2)]=\frac{1}{1-K}(p_2p_9+p_2p_{11}+p_2p_{13}+p_2p_{14}+p_4p_9+p_6p_9+p_7p_9)$$

$$p_3^{\star}=m^{\star}(C_3)=\frac{1}{1-K}[m(C_3)\,g(C_3)+m(C_3)\,g(\{C_1,C_3\})+m(C_3)\,g(\{C_2,C_3\})+m(C_3)\,g(\{C_1,C_2,C_3\})+\ m(\{C_1,C_3\})g(C_3)+\ m(\{C_2,C_3\})g(C_3)+m(\{C_1,C_2,C_3\})g(C_3)]=\frac{1}{1-K}(p_3p_{10}+p_3p_{12}+p_3p_{13}+p_3p_{14}+p_5p_{10}+p_6p_{10}+p_7p_{10})$$

$$p_4^{\star}=m^{\star}(\{C_1,C_2\})=\frac{1}{1-K}[\,m(\{C_1,C_2\})\,g(C_1)+m(\{C_1,C_2\})\,g(C_2)+m(\{C_1,C_2\})\,g(\{C_1,C_2\})+m(\{C_1,C_2\})\,g(\{C_1,C_2,C_3\})+\ m(C_1)g(\{C_1,C_2\})+m(C_2)g(\{C_1,C_2\})+m(\{C_1,C_2,C_3\})g(\{C_1,C_2\})]=\frac{1}{1-K}(p_4p_8+p_4p_9+p_4p_{11}+p_4p_{14}+p_1p_{11}+p_2p_{11}+p_7p_{11})$$

$$p_5^{\star}=m^{\star}(\{C_1,C_3\})=\frac{1}{1-K}[\,m(\{C_1,C_3\})\,g(C_1)+m(\{C_1,C_3\})\,g(C_3)+m(\{C_1,C_3\})\,g(\{C_1,C_3\})+m(\{C_1,C_3\})\,g(\{C_1,C_2,C_3\})+\ m(C_1)g(\{C_1,C_3\})+m(C_3)g(\{C_1,C_3\})+m(\{C_1,C_2,C_3\})g(\{C_1,C_3\})]=\frac{1}{1-K}(p_5p_8+p_5p_{10}+p_5p_{12}+p_5p_{14}+p_1p_{12}+p_3p_{12}+p_7p_{12})$$

$$p_6^{\star}=m^{\star}(\{C_2,C_3\})=\frac{1}{1-K}[\,m(\{C_2,C_3\})\,g(C_2)+m(\{C_2,C_3\})\,g(C_3)+m(\{C_2,C_3\})\,g(\{C_2,C_3\})+m(\{C_2,C_3\})\,g(\{C_1,C_2,C_3\})+\ m(C_2)g(\{C_2,C_3\})+m(C_3)g(\{C_2,C_3\})+m(\{C_1,C_2,C_3\})g(\{C_2,C_3\})]=\frac{1}{1-K}(p_6p_9+p_6p_{10}+p_6p_{13}+p_6p_{14}+p_2p_{13}+p_3p_{13}+p_7p_{13})$$

$$p_7^{\star}=m^{\star}(\{C_1,C_2,C_3\})=\frac{1}{1-K}[\,m(\{C_1,C_2,C_3\})\,g(C_1)+m(\{C_1,C_2,C_3\})\,g(C_2)+m(\{C_1,C_2,C_3\})\,g(C_3)+m(\{C_1,C_2,C_3\})\,g(\{C_1,C_2\})+m(\{C_1,C_2,C_3\})g(\{C_1,C_3\})+\ m(\{C_1,C_2,C_3\})g(\{C_2,C_3\})+m(\{C_1,C_2,C_3\})g(\{C_1,C_2,C_3\})]=\frac{1}{1-K}(p_7p_8+p_7p_9+p_7p_{10}+p_7p_{11}+p_7p_{12}+p_7p_{13}+p_7p_{14})$$

APPENDIX B

Algorithm 1: S-I Perimeter Coverage

Initialize:
S = {S_1,S_2, ..., S_i}: Set of sensor nodes
I = {I_1, I_2, ..., I_j}: Set of interference sources
r_s: Sensing radius of sensor nodes
r_i: Interference radius of interference sources
For each sensor node S_i in S do
Initialize Coverage Status [S_i] to 0
Covered Segments is initially empty
For each sensor node S_j in S, j ≠ i do
If distance (S_i, S_j) ≤ 2 * r_s then
Calculate the segment of Si covered by S_j
Add this segment to Covered Segments
End If
End For
Sort the segments in Covered Segments
Calculate the coverage frequency for S_i based on the sorted segments
End For
For each sensor node S_i in S do
Interference Segments is initially empty
For each interference source I_j in I do
If distance (S_i, I_j) ≤ r_s + r_i then
Calculate the interference segment on S_i due to I_j
Add this segment to Interference Segments
End If
End For
Combine the interference segments with the original covered segments
Recalculate the final coverage status for S_i considering the interference
End for
Return:
return the final coverage status of all sensor nodes

Algorithm 2: Calculate MSR_p Coverage Count

Initialize:
Let S_i be the sensor node under consideration.
Let MSR_p be a segment related to the boundary of node S_i.
Compute:
For each MSR_p associated with node S_i:
If MSR_p is on the inner side of the boundary:
$Q_s = N_{S_{seg}} + 1$ // $N_{S_{seg}}$ is the count of sensor nodes covering the segment S_{seg}.
Else if MSR_p is on the outer side of the boundary:
$Q_s = N_{S_{seg}}$.
End If.
End For.
Return:
Q_s // Return the coverage count for the segment MSR_p.

Algorithm 3: Calculate MSR_q Interference Count

Initialize:
Let S_i be the sensor node under consideration.
Let MSR_q be a segment related to the boundary of node S_i.
Compute:
For each MSR_q associated with node S_i:
If MSR_q is on the inner side of the boundary:
$G_i = N_{I_{seg}} + 1$ // $N_{I_{seg}}$ is the count of sensor nodes covering the segment I_{seg}
Else if MSR_p is on the outer side of the boundary:
$G_i = N_{I_{seg}}$.
End If
End For.
Return:
G_i // Return the coverage count for the segment MSR_p.

APPENDIX C

TABLE I. COVERAGE COUNT STATISTICS FOR S_3 PERIMETER

Perimeter Segment	Sensory Node Coverage Count	Interference Source Coverage Count
$[\alpha_{5,L}, \alpha_{2,R}]$	1	3
$[\alpha_{2,L}, \alpha_{9,R}]$	2	2
$[\alpha_{9,L}, \alpha_{2,R}]$	1	2
$[\alpha_{2,L}, \alpha_{10,R}]$	0	1
$[\alpha_{10,L}, \alpha_{4,R}]$	1	1
$[\alpha_{4,L}, \alpha_{10,R}]$	2	2
$[\alpha_{10,L}, \alpha_{5,R}]$	1	2
$[\alpha_{5,L}, \alpha_{4,R}]$	2	3
$[\alpha_{4,L}, \alpha_{9,R}]$	1	3
$[\alpha_{9,L}, \alpha_{5,R}]$	2	3