This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

Local Threshold Design for Target Localization using Error Correcting Codes in Wireless Sensor Networks in the Presence of Byzantine Attacks

Chun-Yi Wei, *Member*, *IEEE*, Po-Ning Chen, *Senior Member*, *IEEE*, Yunghsiang S. Han, *Fellow*, *IEEE*, and Pramod K. Varshney, *Fellow*, *IEEE*

***Abstract*—In this paper, we revisit the received signal strength (RSS) based target localization technique presented in [1], where a simple threshold quantizer was employed to quantize the RSS values prior to sending them to the fusion center. It was shown that the probability of misclassification of the distributed classification fusion using error correcting codes (DCFECC) scheme vanishes as the number of sensors tends to infinity. This result was obtained based on an intuitive threshold design at the local sensors, and the question of how much a careful design of local thresholds can help improve the overall performance was not addressed. In this work, we demonstrate the significance of threshold design for accurate and robust target localization in wireless sensor networks, particularly when the number of sensors is finite. With this objective, we derive an upper bound on the probability of misclassification as a function of RSS thresholds by using the union inequality. The RSS thresholds that algorithmically minimize the derived misclassification error bound are then numerically obtained over a mirror-based homomorphic sensor deployment structure. Simulations over fading wireless links show that the scheme based on newly found optimized RSS thresholds considerably outperforms the previous scheme using the thresholds that are intuitively selected, especially in the presence of Byzantine attacks that severely impact information security.**

***Index Terms*—Target Localization, Wireless Sensor Networks, Error Correcting Codes, Byzantines, Quantizer Design**

I. Introduction

Target localization has become an important application of the wireless sensor network (WSN) framework. In state-of-the-art techniques, angle of arrival (AOA), time of arrival (TOA) and time difference of arrival (TDOA) are extensively exploited [2], [3], [4], [5], [6]. The AOA approach exploits the arrival angles between neighboring sensors in order to estimate the location of a target. As such, it requires an antenna array, which is generally considered expensive, and hence is not suitable for a low-cost system. As their names suggest, the TOA approach measures the signal propagation time among sensor nodes, and the TDOA approach computes the time difference of the signals propagated between the target and the sensor nodes with known locations. Thus, TOA and TDOA systems yield inaccurate target localization if reliable synchronization among sensor nodes cannot be established [7], [8], [9]. This motivates us to direct our attention on an alternate received signal strength (RSS) based approach for target localization which has low power consumption, low cost and low complexity.

The RSS based target localization technique usually confines its target search within a region of interest (ROI), which is sub-divided into multiple segmented areas. The sensors are often deployed equally over these areas, and they constantly monitor the channel through which the target emits its signal. Once the sensor nodes capture the signal radiated from the target, they quantize the received signal strength (RSS) and transmit either quantized outputs [10] or local decisions to the fusion center (FC) through noisy wireless links. By using methodologies such as least-square or maximum-likelihood [11], [12], an estimate of the target location is determined by the FC.

In addition to signal corruption due to sensing noise and imperfection of wireless links, the accuracy of target localization can be seriously diminished by malicious Byzantine attacks [13], [14], [15], where the so-called Byzantine attacks or data falsification attacks considered here are adversarial actions to compromise the sensors and deliberately lead the sensors to report faulty data bits to the FC. The FC even becomes blind to the target when the fraction of Byzantine sensors is higher than 50% [16]. A straightforward mitigation of Byzantine adversaries is to identify Byzantine sensors and exclude their faulty information [16]. Another mitigation approach is to introduce fault-tolerance capability into system design. In either case, error correcting coding techniques can be employed to assist in detecting and correcting the corrupted data bits [17].

This resulted in the contribution of [18], [19], [20], where the distributed classification fusion using error correcting codes (DCFECC) paradigm was shown to be effective in mitigating the impact of Byzantine attacks. The idea is to associate each class, defined according to which segmentation region the target is located in, with a codeword that is

This work was supported in part by the National Science of Council (NSC) of Taiwan under Grants NSC 102-2221-E-011-006-MY3, NSC 101-2221-E-011-069-MY3 and by ARO grant W911NF-14-1-0339.

C.-Y. Wei is with the Dept. of Communication Engineering, National Taipei University, New Taipei City, Taiwan (email: cywei@gm.ntpu.edu.tw).

P.-N. Chen is with the Inst. of Communications Engineering & Dept. of Electrical and Computer Engineering, National Chiao-Tung University, Hsinchu City, Taiwan (email: poning@faculty.nctu.edu.tw).

Y. S. Han is with the School of Electrical Engineering & Intelligentization, Dongguan University of Technology, Dongguan, P. R. China (email: yunghsiangh@gmail.com).

P. K. Varshney is with the Dept. of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY 13244, USA (e-mail: varshney@syr.edu).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

transmitted from sensors to the FC in parallel. By decoding the receptions from the sensors and determining the most likely codeword to be transmitted, the FC pinpoints the region that the target is possibly located in. It should be noted that the messages transmitted from sensors to the FC may also be interfered by channel noise and fading of the wireless links in addition to Byzantine attacks, making the receptions deviate from the correct codeword. By taking the majority of individual decisions of all the sensors, correction of certain deviations from the correct codeword can be achieved.

On top of a multi-layer hierarchical DCFECC system, iterative classification was further proposed in [1]. At each iteration, the ROI, where the target may be located, is split into L non-overlapping *super-regions* consisting of multiple segmented regions. Based on DCFECC, the FC selects the super-region, where the target is most likely located, inside the current ROI. The FC then sets the super-region just selected to be the ROI of the next iteration. Only the sensors in the current ROI need to report their decisions to the FC. Thus, the number of sensors involved at each iteration can be rapidly decreased by a factor of L. As a result, this sophisticated design of iterative classification over a multi-layer hierarchical DCFECC system not only retains the desired robustness to sensor faults due to Byzantine attacks but considerably reduces the decoding complexity for target localization.

Since each sensor is required to only report a binary decision to the FC, a simple threshold quantizer on the received signal strength (RSS) was adopted in [1], where a "1" was reported if the RSS was larger than the threshold, and a "0" was sent, otherwise. With a threshold inversely proportional to the distance between the sensor and the center of the segmentation region that the sensor lies in, it was shown in [1] that such a simple system design can achieve an asymptotically vanishing probability of misclassification as the number of sensors grows to infinity even under a moderately high degree of Byzantine attacks.

Although the intuitive threshold design in [1] has been shown to perform well asymptotically, numerical experiments suggest that they are by no means optimal when the number of sensors is fixed and finite. A research direction of practical interest then arises as to how significant an elaborate design of local thresholds is for an accurate and robust target localization in WSNs of finite size.

With this objective in mind, determination of the local thresholds that minimize the detection error for identification of the ROI that the target is located in becomes a natural target to pursue. Since under the non-asymptotic (in number of sensors) iterative classification scenario we consider, an exact expression of the detection error for target localization cannot be obtained, an assumption on sensor deployment structure, where the locations of sensors in different super-regions are guaranteed to be mirror-based homomorphic, is imposed in this paper. Based on the assumption, a union bound as a function of RSS thresholds can be derived. This union bound is then used as an objective function for the numerical determination of the best RSS thresholds. Simulation results show that taking the bound we derive as an objective function results in a set of thresholds that considerably outperform the intuitive ones adopted in [1], especially when Byzantine attacks are present.

In summary, the main contributions of this paper are as follows:

1) Based on the union inequality and the particular mirror-based homomorphic sensor deployment structure we consider in this paper, an upper bound on the probability of misclassification is derived as a function of RSS thresholds. Since the bound is quite accurate at high signal-to-noise ratios, the resulting thresholds are near-optimal in the sense of minimizing the misclassification probability. These thresholds then lead to a new insight in that a sensor closer to the boundary between two super-regions should have a larger threshold which is in stark contrast to the intuition adopted in [1] where larger thresholds were assigned to sensors closer to the center of a super-region instead of its boundary.
2) The derived objective function based on the misclassification probability bound considerably simplifies the computational complexity of searching for the most suitable thresholds for local sensors. The obtained thresholds are applicable to practical WSNs with finite number of sensors.

The rest of the paper is structured as follows. Section II reviews the work related to the problem considered in this paper while Section III defines the system model. The DCFECC scheme and its hard/soft-decision decoding as well as iterative classification on top of a multi-layer hierarchical DCFECC system are introduced in Section IV. Analysis of bounds on the probability of misclassification is given in Section V. The numerical algorithm to determine the suitable RSS thresholds based on the derived upper bound on misclassification error is presented in Section VI. Section VII then presents and discusses the simulation results, and Section VIII concludes the work.

II. Related Work

As aforementioned, a straightforward solution for the Byzantine adversary problem is to identify the Byzantine sensors and exclude the faulty information received from them [16]. This, however, may be a tough challenge under certain circumstances and hence fault-tolerance capability has to be introduced into system design. An example is the contribution of [21], where a fault-tolerant localization algorithm, referred to as Subtract on Negative Add on Positive (SNAP), was proposed. The SNAP algorithm employed a likelihood function to determine the most likely ROI through the sensing information from sensors.[1] Because only the sensors in an ROI can contribute to the likelihood function values, the faulty sensors outside the ROI will not affect the accuracy of target localization, and hence negative impact from faulty sensors can be mitigated. The authors of [21] further proposed a two-phase localization procedure for their SNAP algorithm in a subsequent work [22], employing SNAP over an identified ROI that the target is hypothesized to be located in, and making

[1]The ROI was called the region of coverage (ROC) in [21].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

possible the tracking of multiple sources. Localization among many overlapping ROIs using SNAP, however, may require intensive computational effort.

As an alternative approach, conventional error control coding techniques have been incorporated into target localization [23]. This approach, although possibly complex at the design stage, can simultaneously compensate for sensing noise and imperfection of wireless links as well as Byzantine attacks without the need to identify the cause of information deterioration as long as the deterioration is within the error correcting capability of the adopted code. An example of this alternative approach is the DCFECC paradigm introduced in [18], where error control codes were successfully employed for distributed inference with corrupted observations.

Techniques for target localization over WSNs can also be extensively used in solving problems of analogous nature such as estimation of the arrival direction of an acoustic wavefront through cooperation of a network of sensors [24], [25], [26]. Another example of such is the distributed source coding scheme in [27], where the lowest achievable sum rate is investigated under the consideration that the data is required to be reconstructed from observations of sensors, of which some may suffer Byzantine attacks.

All the works mentioned above handle the task of target localization at the physical layer. In certain situations, message exchanges among nearby sensors, which is more likely to be conducted at the network layer,[2] is a more favored approach for target localization, in particular over a large-scale wireless sensor network where direct communication from the sensors to the FC is not always available [29]. Along this research direction, the authors in [30] provide an excellent framework for a *large-scale* wireless sensor network that takes into account the constraint from a class of bounded-height tree topologies from [31]. An optimal distributed fusion protocol, which allows the messages to be transmitted from a parent sensor node to a child sensor node, and which can efficiently reach a consensus among sensors after a certain number of message exchanges, was established [30].

In a situation where sensor networks have no FC, a cross-layer approach for target localization has been proposed in [32], in which the sensors are assumed to have the capability to communicate with neighboring sensors. In the framework considered in [32], sensors exchange weighted likelihood function values of their observations with neighboring sensors, and the target location is finalized when sensors reach a consensus after multiple message exchanges.

In contrast to finding the optimal message-exchange protocol subject to network topology constraints, target localization that we consider in this paper is conducted at the physical layer due to the unavailability of a protocol stack at local sensors [7], [8], [9]. Only simple analog measurements are acquired at the physical layer of sensors and are utilized for the estimation of target location. As a result of limited resources such as energy and bandwidth, sensors are allowed to transmit only a small number of bits to the FC. Therefore, in the particular framework that we consider in this paper, using a multiple-step message-exchange algorithm is impractical. Similar consideration can also be seen in related publications such as [1], [7], [8], [9], where only binary or multiple-bit quantized data was transmitted from local sensors to the FC. This follows the system model defined in the next section.

[2]It is also possible to have message exchanges among a group of specific sensors using beamforming techniques at the physical layer [28], which allows a transmission device to steer its signal along a particular direction. However, in applications that deploy inexpensive sensors with limited resources such as energy and realization cost, to equip the sensors with beamforming devices may not be cost-economical.

III. System Model

The WSN scenario discussed in this paper is described as follows. In a designated ROI $\mathcal{R}$, there are N cooperating sensors deployed to estimate the location of a target. The location of the target is denoted by $\boldsymbol{\theta} = (\boldsymbol{x}, \boldsymbol{y})$,[3] where $(\boldsymbol{x}, \boldsymbol{y})$ represents the random coordinates of the target in a 2-dimensional Cartesian plane. Likewise, $\theta_i = (x_i, y_i)$ characterizes the position of the ith sensor for $1 \leq i \leq N$. It is assumed that the locations of the sensors are known to the FC and the sensors constantly monitor the channel through which the target radiates its signal. The signal received by the ith sensor is modeled by

$$\boldsymbol{s}_i = \boldsymbol{a}_i + \boldsymbol{n}_i \quad \text{for } i = 1, 2, \ldots, N, \tag{1}$$

where $\boldsymbol{a}_i$ denotes the noise-free signal received at the ith sensor, and $\boldsymbol{n}_i$ is the noise experienced during the sensing operation. We assume that $\{\boldsymbol{a}_i\}_{i=1}^N$ and $\{\boldsymbol{n}_i\}_{i=1}^N$ are independent of each other, and the latter are independent and identically distributed (i.i.d.) Gaussian random variables with mean zero and variance σ^2. Furthermore, $\boldsymbol{a}_i$ follows the inverse-square law of radiation as

$$\boldsymbol{a}_i^2 = P_0 \left(\frac{d_0}{\boldsymbol{d}_i}\right)^2 \text{ for } i = 1, 2, \ldots, N, \tag{2}$$

where P_0 is the power measured at the reference distance d_0,[4] and

$$\boldsymbol{d}_i = d_{\mathrm{E}}(\boldsymbol{\theta}, \theta_i) = \sqrt{(\boldsymbol{x} - x_i)^2 + (\boldsymbol{y} - y_i)^2}$$

is the Euclidean distance between the target and the ith sensor. Thus, random variables $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_N$ are generally dependent due to their common dependence on $\boldsymbol{\theta} = (\boldsymbol{x}, \boldsymbol{y})$.

In the scheme presented in [1], sensors only return binary decisions to the FC due to their limited bandwidth, and these decisions are made based on simple threshold rules corresponding to whether the target is within a certain range or not. Thus, the decision $\boldsymbol{u}_i$ made by the ith sensor is controlled by the local threshold η_i for this sensor and follows

$$\boldsymbol{u}_i = \begin{cases} 0, & \boldsymbol{s}_i \leq \eta_i; \\ 1, & \boldsymbol{s}_i > \eta_i. \end{cases} \tag{3}$$

[3]Throughout the paper, both $\boldsymbol{\theta}$ and $(\boldsymbol{x}, \boldsymbol{y})$ are used to denote the location of the target, depending on the ease of representation. In addition, as a convention, underlined letters denote vectors; boldface letters such as $\boldsymbol{u}_i$ and $\underline{\boldsymbol{u}} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_N)$ respectively denote random variables and random vectors; and non-boldface letters such as u_i and $\underline{u} = (u_1, u_2, \ldots, u_N)$ are their realizations.

[4]In this work, all the Euclidean distances are measured in the same unit as (and also with respect to) the reference distance d_0. For convenience, we let $d_0 = 1$ meter. As an example, the performance index of mean square error (MSE) presented later will be measured in the unit of meter square.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

The noisy link between the ith sensor and the FC is modeled as

$$\boldsymbol{v}_i = \boldsymbol{h}_i(-1)^{\boldsymbol{u}_i}\sqrt{\mathrm{E_b}} + \boldsymbol{w}_i, \tag{4}$$

where $\boldsymbol{h}_i$ denotes the unit-variance Rayleigh distributed fading attenuation of the wireless link, $\mathrm{E_b}$ is the energy required to transmit one sensor bit, and $\boldsymbol{w}_i$ is the additive Gaussian noise corresponding to the wireless link. Here, we assume that $\boldsymbol{w}_i$ has mean zero and variance σ_{w}^2. In addition, $\{\boldsymbol{h}_i\}_{i=1}^N$ and $\{\boldsymbol{w}_i\}_{i=1}^N$ are both i.i.d. and are independent of each other.

IV. Distributed Classification Fusion using Error Correcting Codes

A. Background

In this section, we revisit Distributed Classification Fusion using Error Correcting Codes (DCFECC) presented in [1]. As proposed therein, the designated region of interest (ROI) $\mathcal{R}$ is partitioned into M regions, which are denoted as $\mathcal{R}_1$, $\mathcal{R}_2$, ..., $\mathcal{R}_M$, and which can be pre-determined by, e.g., a Voronoi diagram associated with a set of given center points $(\bar{\theta}_1, \bar{\theta}_2, \ldots, \bar{\theta}_M)$. The hypothesis corresponding to the target lying in region $\mathcal{R}_\ell$ (i.e., $\boldsymbol{\theta} \in \mathcal{R}_\ell$) is denoted as $H_{\ell-1}$. Upon the reception of the signals from the target, the N local sensors transmit their binary decisions to the FC, whose action is to determine which region the target is located in.

In the DCFECC scheme, an M-by-N binary code matrix $\mathbb{C}$ is generated to assist in determining the region that the target resides in. For $1 \le \ell \le M$, the ℓth row of $\mathbb{C}$ is associated with hypothesis $H_{\ell-1}$, where subject to $\boldsymbol{\theta} \in \mathcal{R}_\ell$, sensors in $\mathcal{R}_\ell$ are anticipated to report "1", while sensors outside $\mathcal{R}_\ell$ are likely to output "0". For $1 \le i \le N$, the ith column of $\mathbb{C}$ indicates the region that the ith sensor belongs to. An example for $M = 4$ and $N = 16$ is given below:

$$\mathbb{C} = \begin{bmatrix} 1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1 \end{bmatrix}, \tag{5}$$

where in the above setting, the first four sensors are located in region $\mathcal{R}_1$, the next four sensors lie in region $\mathcal{R}_2$, sensor 9 to sensor 12 are inside region $\mathcal{R}_3$ and the last four sensors reside in region $\mathcal{R}_4$. We will use $\mathcal{S}_\ell$ to denote the set of indices of sensors in region $\mathcal{R}_\ell$; hence, in the above example, $\mathcal{S}_1 = \{1, 2, 3, 4\}$, $\mathcal{S}_2 = \{5, 6, 7, 8\}$, $\mathcal{S}_3 = \{9, 10, 11, 12\}$ and $\mathcal{S}_4 = \{13, 14, 15, 16\}$. Also, the element of $\mathbb{C}$ in the ℓth row and the ith column is denoted as $c_{\ell,i}$, while codeword $\underline{c}_\ell$ is a shorthand for $(c_{\ell,1}, c_{\ell,2}, \ldots, c_{\ell,N})$. Based on the code matrix, the FC can determine which hypothesis should be declared true by using either a hard-decision decoding algorithm or a soft-decision one, which will be introduced in next section.

B. Decoding Schemes for Distributed Classification

Based on the reception $\underline{\boldsymbol{v}} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_N)$ defined by (4), the FC computes their corresponding log-likelihood ratios as

$$\xi_i = \ln \frac{f(\boldsymbol{v}_i = v_i | u_i = 0)}{f(\boldsymbol{v}_i = v_i | u_i = 1)}, \quad i = 1, 2, \ldots, N,$$

where $f(\boldsymbol{v}_i|u_i)$ is the probability density function (pdf) obtained from the respective Rayleigh fading channel model. A hard-decision decoding based FC then transforms each ξ_i to its hard-decision counterpart according to $\kappa_i = \mathbf{1}(\xi_i \le 0)$, where $\mathbf{1}(\cdot)$ is the set indicator function, and determines the region $\mathcal{R}_{\hat{\ell}}$ that the target belongs to using the minimum Hamming distance fusion rule [17], i.e.,

$$\hat{\ell} = \arg \min_{1 \le \ell \le M} d_{\mathrm{H}}(\underline{\kappa}, \underline{c}_\ell) \tag{6}$$

with $\underline{\kappa} = (\kappa_1, \kappa_2, \ldots, \kappa_N)$, where $d_{\mathrm{H}}(\cdot, \cdot)$ is the Hamming distance.

It, however, was shown in [33] that the hard-decision decoding performance of the DCFECC scheme deteriorates when channel fading is introduced. Hence, a Distributed Classification using Soft-decision Decoding (DCSD) scheme was proposed therein and shown to outperform the hard-decision decoding based DCFECC in the presence of channel fading. Because the soft-decision decoder given in [1, Eq. (6)] may be computationally intensive, a simplification was subsequently devised in [1, Eq. (43)]. As a result of such simplification, the most likely region that the target belongs to is decided by finding the row of $\mathbb{C}$ that is closest to the likelihood ratio vector $\underline{\xi} = (\xi_1, \xi_2, \ldots, \xi_N)$ in Euclidean distance, i.e.,

$$\hat{\ell} = \arg \min_{1 \le \ell \le M} d_{\mathrm{E}}(\underline{\xi}, (-1)^{\underline{c}_\ell}), \tag{7}$$

where $d_{\mathrm{E}}(\underline{\xi}, (-1)^{\underline{c}_\ell}) \triangleq \sum_{i=1}^N (\xi_i - (-1)^{c_{\ell,i}})^2$ is the Euclidean distance.

C. Iterative Classification

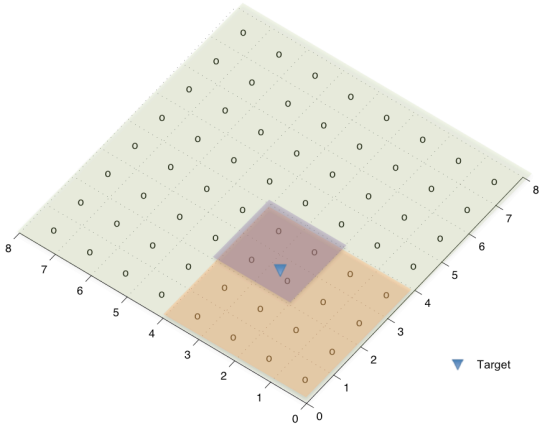


Fig. 1. Illustration of iterative classification on top of a three-layer hierarchical DCFECC system with $N = 64$ sensors, where each layer consists of only $L = 4$ super-regions as in contrast to a total of $M = 16$ regions. Here, "○" denotes the locations of sensors.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

The decoding based DCFECC not only simplifies the decision making process at the FC, particularly in comparison with the traditional maximum likelihood estimation, but is also resilient to sensor faults due to Byzantine attacks as well as channel impairments. The decoding effort in both (6) and (7), however, requires MN metric computations, which grows considerably when the number of sensors is moderately large. In order to obtain a computationally efficient classification scheme, the authors in [1] further proposed an iterative classification framework on top of a hierarchical DCFECC system.

The idea behind the iterative classification in [1] can be described as follows. At each iteration, the ROI is split into L non-overlapping super-regions with L being possibly much smaller than the total number of regions M. As an example illustrated in Figure 1, given a three-layer hierarchical DCFECC system with $N = 64$ sensors that are equally distributed over $M = 16$ regions, the ROI is split into $L = 4$ non-overlapping super-regions at each iteration. An L-ary hypothesis test is then performed at the FC to determine the super-region that the target is most likely located in at each iteration. The decision is then regarded as the new ROI for the next classification iteration. Through such a hierarchical zoom-in process, the area of ROI is reduced by a factor of L at each iteration, and the region that the target belongs to is determined eventually. Notably, only the sensors in the current ROI need to report their local decisions to the FC. Because the ROI is downsized by a multiplicative factor of $(1/L)^k$ after k iterations, the number of equally distributed sensors required to report their local decisions to the FC is proportionally reduced; hence, the code size and codeword length can be considerably downscaled at each iteration and the decoding complexities are much reduced. This reduction can be substantiated again by the example in Figure 1, where $MN = 16 \times 64 = 1,024$ metric computations can be reduced to $LN + L(N/L) + L(N/L^2) = 4 \times 64 + 4 \times 16 + 4 \times 4 = 336$ metric computations. More saving in computational efforts can be obtained when the number of sensors further increases.

We next define the notations that will be used in later performance analysis for iterative classification. Denote the number of sensors required to report their local decisions to the FC at the kth iteration by $N_k \triangleq N/L^{k-1}$ for $1 \leq k \leq k_{\text{stop}}$, where k_{stop} is the maximum number of iterations, and the code matrix used at the FC at the kth iteration becomes of size $L \times N_k$. We use the notation $\mathbb{C}^k$ to denote the code matrix used at the kth iteration and denote its ℓth row by $\underline{c}_\ell^k = (c_{\ell,1}^k, c_{\ell,2}^k, \ldots, c_{\ell,N_k}^k)$ for $1 \leq \ell \leq L$. By following the same notational convention, the L super-regions obtained by subdividing the ROI at the kth iteration are denoted as $\mathcal{R}_1^k, \mathcal{R}_2^k, \ldots, \mathcal{R}_L^k$, and let $\mathcal{R}^k \triangleq \cup_{\ell=1}^L \mathcal{R}_\ell^k$; the center points corresponding to these super-regions are denoted as $\bar{\theta}_1^k, \bar{\theta}_2^k, \ldots, \bar{\theta}_L^k$; the set of indices of sensors belonging to super-region $\mathcal{R}_\ell^k$ is denoted as $\mathcal{S}_\ell^k \triangleq \{i \in \mathcal{N} : \theta_i \in \mathcal{R}_\ell^k\}$, where $\mathcal{N} \triangleq \{1, 2, \ldots, N\}$, and $\mathcal{S}^k \triangleq \cup_{\ell=1}^L \mathcal{S}_\ell^k$; the local threshold used by the ith sensor at the kth iteration is denoted by η_i^k; and the local decision transmitted to the FC from the ith sensor at the kth iteration is denoted by $\boldsymbol{u}_i^k = \mathbf{1}(\boldsymbol{s}_i > \eta_i^k)$, where $\mathbf{1}(\cdot)$ is the set indicator function. In addition, by dropping its dependence on the iteration number, we use a convenient shorthand notation $r(i)$ (rather than $r^k(i)$) to identify the index of the super-region that the ith sensor is located in, i.e., $r(i) = \ell$ if $i \in \mathcal{S}_\ell^k$. Note that the system does not need to re-sense the signal radiated from the target at each iteration but simply to re-perform binary quantization according to the iteratively updated thresholds; hence, superscript k is not necessary for $\{\boldsymbol{s}_i\}_{i=1}^N$.

With these notations, the problem pursued in this work is that instead of intuitively setting the local threshold η_i^k in (3) to be $\sqrt{P_0}/d_{\text{E}}(\theta_i, \bar{\theta}_{r(i)}^k)$ as in [1], we devise a strategy to determine a better threshold η_i^k in order to improve system performance. Details will be given in subsequent sections.

V. Performance analysis under ideal wireless links

In this section, we derive a bound on the probability of misclassification for iterative localization under the assumption of ideal wireless links. As far as we know, no closed-form expression of the probability of detection error for iterative localization has been derived in the literature. Often in similar situations in the coding literature, a bound based on the union inequality is employed when an exact analysis of the error performance cannot be carried out. We employ a similar approach to derive the bound for our problem and then use it as an objective function for the optimization of the thresholds used by local sensors.

As previously mentioned, the FC conducts an L-ary hypothesis test iteratively. Thus, a misclassification occurs if the target is not within the super-region of the declared hypothesis at any iteration. In this section, we derive an upper bound on this misclassification probability. This upper bound will then be used to determine the local thresholds $\{\eta_i^k\}_{i=1}^{N_k}$ that result in a better performance than the ones proposed in [1] in the next section.

For simplicity, we assume an ideal wireless link between the FC and the sensors, i.e., $\boldsymbol{h}_i = 1$ and $\boldsymbol{w}_i = 0$ with probability one in (4). Thus, the FC can perfectly recover $\boldsymbol{u}_i$ for every i in $\mathcal{S}^k$. Under this assumption, we can replace (7) by the minimum Hamming distance criterion [17], based on which the decision regions for the ℓth codeword at the kth iteration are given by

$$\mathcal{D}_\ell^{k,+} = \left\{ \underline{u}^k \in \{0,1\}^{N_k} \ : \ d_{\text{H}}(\underline{u}^k, \underline{c}_\ell^k) \leq \min_{1 \leq j \leq L} d_{\text{H}}(\underline{u}^k, \underline{c}_j^k) \right\}$$

and

$$\mathcal{D}_\ell^{k,-} = \left\{ \underline{u}^k \in \{0,1\}^{N_k} \ : \ d_{\text{H}}(\underline{u}^k, \underline{c}_\ell^k) < \min_{1 \leq j \leq L, \ j \neq \ell} d_{\text{H}}(\underline{u}^k, \underline{c}_j^k) \right\}$$

for $1 \leq \ell \leq L$, where $d_{\text{H}}(\cdot, \cdot)$ is the Hamming distance.

According to their definitions, the set of $\mathcal{D}_\ell^{k,+}$ consists of the received vectors that are at least as close to $\underline{c}_\ell^k$ as to any other codewords, where received vectors that are of equal Hamming distance to $\underline{c}_\ell^k$ and to some other codeword are all included, while $\mathcal{D}_\ell^{k,-}$, as a subset of $\mathcal{D}_\ell^{k,+}$, is formed by excluding all elements in $\mathcal{D}_\ell^{k,+}$ that could cause a tie decision.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

Observe that $\{\boldsymbol{d}_i = d_{\rm E}(\boldsymbol{\theta}, \theta_i)\}_{i\in\mathcal{S}^k}$ are generally dependent random vectors because of their dependence on the common random location of the target $\boldsymbol{\theta}$, and so are $\{\boldsymbol{a}_i = \sqrt{P_0}/\boldsymbol{d}_i\}_{i\in\mathcal{S}^k}$. This implies that both $\{\boldsymbol{s}_i = \boldsymbol{a}_i + \boldsymbol{n}_i\}_{i\in\mathcal{S}^k}$ and $\{\boldsymbol{u}_i^k = \mathbf{1}(\boldsymbol{s}_i > \eta_i^k)\}_{i\in\mathcal{S}^k}$ are dependent across sensors. To overcome the impact of this dependency, we notice that for a given $\boldsymbol{\theta} = \theta$, $\{d_i = d_{\rm E}(\theta, \theta_i)\}_{i\in\mathcal{S}^k}$ and $\{a_i = \sqrt{P_0}/d_i\}_{i\in\mathcal{S}_k}$ become constants, by which the statistical dependencies in $\{\boldsymbol{s}_i = a_i + \boldsymbol{n}_i\}_{i\in\mathcal{S}^k}$ and $\{\boldsymbol{u}_i^k = \mathbf{1}(\boldsymbol{s}_i > \eta_i^k)\}_{i\in\mathcal{S}^k}$ can be conditionally removed. This observation is the basis of our analysis.

Let $P_{\rm e}^k$ be the probability of misclassification at the kth iteration, subject to the premise that the target is contained in $\mathcal{R}^k$. Then irrespective of ties, $P_{\rm e}^k$ can be upper- and lower-bounded by

$$\begin{aligned}\sum_{\ell=1}^{L} \pi_{\ell-1}^k \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,-} \middle| H_{\ell-1}^k\right) &\geq P_{\rm e}^k \\ &\geq \sum_{\ell=1}^{L} \pi_{\ell-1}^k \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,+} \middle| H_{\ell-1}^k\right), \end{aligned} \tag{8}$$

where $\pi_{\ell-1}^k = \Pr(\boldsymbol{\theta} \in \mathcal{R}_\ell^k)$ is the prior probability that hypothesis $H_{\ell-1}^k = [\boldsymbol{\theta} \in \mathcal{R}_\ell^k]$ is true, subject to $\boldsymbol{\theta} \in \mathcal{R}^k$. We thus derive

$$\begin{aligned}&\pi_{\ell-1}^k \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,+} \middle| H_{\ell-1}^k\right) \\ &= \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,+} \wedge \boldsymbol{\theta} \in \mathcal{R}_\ell^k\right) \\ &= \int_{\mathcal{R}} \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,+} \wedge \theta \in \mathcal{R}_\ell^k \middle| \boldsymbol{\theta} = \theta\right) dF^k(\theta) \\ &= \int_{\mathcal{R}_\ell^k} \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,+} \middle| \boldsymbol{\theta} = \theta\right) dF^k(\theta),\end{aligned}$$

where $F^k(\cdot)$ is the cumulative distribution function (cdf) of $\boldsymbol{\theta}$ given that it belongs to $\mathcal{R}^k$. Similarly,

$$\pi_{\ell-1}^k \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,-} \middle| H_{\ell-1}^k\right) = \int_{\mathcal{R}_\ell^k} \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,-} \middle| \boldsymbol{\theta} = \theta\right) dF^k(\theta).$$

As a result, (8) can be rewritten as

$$\begin{aligned}&\sum_{\ell=1}^{L} \int_{\mathcal{R}_\ell^k} \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,-} \middle| \boldsymbol{\theta} = \theta\right) dF^k(\theta) \\ &\geq P_{\rm e}^k \geq \sum_{\ell=1}^{L} \int_{\mathcal{R}_\ell^k} \Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,+} \middle| \boldsymbol{\theta} = \theta\right) dF^k(\theta).\end{aligned}$$

We then infer from the structure of our code matrix (see, for example, (5)) that

$$\begin{aligned}&d_{\rm H}(\underline{u}^k, \underline{c}_\ell^k) \geq d_{\rm H}(\underline{u}^k, \underline{c}_j^k) \\ &\iff \sum_{i\in\mathcal{S}_\ell^k} (u_i^k \oplus c_{\ell,i}^k) + \sum_{i\in\mathcal{S}_j^k} (u_i^k \oplus c_{\ell,i}^k) \\ &\qquad \geq \sum_{i\in\mathcal{S}_\ell^k} (u_i^k \oplus c_{j,i}^k) + \sum_{i\in\mathcal{S}_j^k} (u_i^k \oplus c_{j,i}^k) \\ &\iff \sum_{i\in\mathcal{S}_\ell^k} (u_i^k \oplus c_{\ell,i}^k) + \sum_{i\in\mathcal{S}_j^k} (u_i^k \oplus c_{\ell,i}^k) \\ &\qquad \geq \sum_{i\in\mathcal{S}_\ell^k} [1 - (u_i^k \oplus c_{\ell,i}^k)] + \sum_{i\in\mathcal{S}_j^k} [1 - (u_i^k \oplus c_{\ell,i}^k)] \\ &\iff \sum_{i\in\mathcal{S}_\ell^k \bigcup \mathcal{S}_j^k} z_{i,\ell}^k \geq 0, \end{aligned} \tag{9}$$

where $z_{i,\ell}^k = 2(u_i^k \oplus c_{\ell,i}^k) - 1$, and "$\oplus$" denotes modulo-2 addition. In light of (9), we proceed to obtain that

$$\begin{aligned}&\Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,-} \middle| \boldsymbol{\theta} = \theta\right) \\ &= \Pr\left(d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_\ell^k) \geq \min_{1\leq j\leq L,\, j\neq\ell} d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_j^k) \middle| \boldsymbol{\theta} = \theta\right) \\ &= \Pr\Big(d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_\ell^k) \geq d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_1^k) \vee \cdots \vee\ d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_\ell^k) \\ &\qquad \geq d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_{\ell-1}^k) \vee\ d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_\ell^k) \geq d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_{\ell+1}^k) \\ &\qquad \vee \cdots \vee\ d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_\ell^k) \geq d_{\rm H}(\underline{\boldsymbol{u}}^k, \underline{c}_L^k) \Big| \boldsymbol{\theta} = \theta\Big) \\ &= \Pr\Big(\sum_{i\in\mathcal{S}_\ell^k \bigcup \mathcal{S}_1^k} \boldsymbol{z}_{i,\ell}^k \geq 0 \vee \cdots \vee \sum_{i\in\mathcal{S}_\ell^k \bigcup \mathcal{S}_{\ell-1}^k} \boldsymbol{z}_{i,\ell}^k \geq 0 \\ &\qquad \vee \sum_{i\in\mathcal{S}_\ell^k \bigcup \mathcal{S}_{\ell+1}^k} \boldsymbol{z}_{i,\ell}^k \geq 0 \\ &\qquad \vee \cdots \vee \sum_{i\in\mathcal{S}_\ell^k \bigcup \mathcal{S}_L^k} \boldsymbol{z}_{i,\ell}^k \geq 0 \ \Big| \boldsymbol{\theta} = \theta\Big) \\ &\leq \sum_{j=1,\, j\neq\ell}^{L} \Pr\Big(\sum_{i\in\mathcal{S}_\ell^k \bigcup \mathcal{S}_j^k} \boldsymbol{z}_{i,\ell}^k \geq 0 \ \Big| \boldsymbol{\theta} = \theta\Big). \end{aligned} \tag{10}$$

Let $q_{i,\ell}^k = q_{i,\ell}^k(\theta) \triangleq \Pr\left(\boldsymbol{z}_{i,\ell}^k = 1 \middle| \boldsymbol{\theta} = \theta\right)$. By noting that $\{\boldsymbol{z}_{i,\ell}^k\}_{i\in\mathcal{S}^\ell \bigcup \mathcal{S}^j}$ are conditionally independent given $\boldsymbol{\theta} = \theta$, we obtain from [34, Lemma 2] that if for every $1 \leq j \leq L$ with $j \neq \ell$,

$$\begin{aligned}\lambda_{\ell,j}^k &\triangleq \frac{L}{2N_k} \sum_{i\in\mathcal{S}_\ell^k \bigcup \mathcal{S}_j^k} E\left[\boldsymbol{z}_{i,\ell}^k\right] = \frac{L}{2N_k} \sum_{i\in\mathcal{S}_\ell^k \bigcup \mathcal{S}_j^k} (2q_{i,\ell}^k - 1) \\ &= \frac{L}{N_k} \sum_{i\in\mathcal{S}_\ell^k \bigcup \mathcal{S}_j^k} q_{i,\ell}^k - 1 \leq 0, \end{aligned} \tag{11}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

then (10) is upper-bounded by[5]

$$\Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,-} \middle| \boldsymbol{\theta}=\theta\right) \leq \sum_{j=1,j\neq\ell}^{L}\left(1-\frac{\left(\sum_{i\in S_\ell^k\cup S_j^k}(2q_{i,\ell}^k-1)\right)^2}{(d_{\min}^k)^2}\right)^{d_{\min}^k/2},$$

where $d_{\min}^k \triangleq 2N_k/L$ is the minimum pairwise Hamming distance of $\mathbb{C}^k$. This concludes that if $\max_{1\leq\ell,j\leq L,\ell\neq j}\lambda_{\ell,j}^k < 0$, the probability of misclassification satisfies

$$P_{\mathrm{e}}^k \leq \sum_{\ell=1}^{L}\int_{\mathcal{R}_\ell^k}\Pr\left(\underline{\boldsymbol{u}}^k \notin \mathcal{D}_\ell^{k,-}\middle|\boldsymbol{\theta}=\theta\right)dF^k(\theta) \leq \sum_{\ell=1}^{L}\int_{\mathcal{R}_\ell^k}\left\{\sum_{j=1,\,j\neq\ell}^{L}\left(1-\frac{\left(\sum_{i\in S_\ell^k\cup S_j^k}(2q_{i,\ell}^k-1)\right)^2}{(d_{\min}^k)^2}\right)^{d_{\min}^k/2}\right\}dF^k(\theta). \quad (13)$$

We next establish the connection between the upper bound in (13) and the thresholds $\{\eta_i^k\}_{i\in\mathcal{S}^k}$. It can be verified that for $i\in\mathcal{S}_\ell^k$,

$$\begin{aligned} q_{i,\ell}^k &= \Pr\left(\boldsymbol{z}_{i,\ell}^k=1\middle|\boldsymbol{\theta}=\theta\right)=\Pr\left(\boldsymbol{u}_i^k\oplus c_{\ell,i}^k=1\middle|\boldsymbol{\theta}=\theta\right)\\ &= \Pr\left(\boldsymbol{u}_i^k=0\middle|\boldsymbol{\theta}=\theta\right)=\Pr\left(\boldsymbol{s}_i<\eta_i^k\middle|\boldsymbol{\theta}=\theta\right)\\ &= \Pr\left(a_i+\boldsymbol{n}_i<\eta_i^k\middle|\boldsymbol{\theta}=\theta\right)\\ &= \Phi\left(\frac{\eta_i^k-a_i}{\sigma}\right), \end{aligned} \quad (14)$$

where $\Phi(\cdot)$ is the cdf of the standard normal distribution. Likewise, for $i\notin\mathcal{S}_\ell^k$,

$$\begin{aligned} q_{i,\ell}^k &= \Pr\left(\boldsymbol{u}_i^k=1\middle|\boldsymbol{\theta}=\theta\right)=\Pr\left(\boldsymbol{s}_i>\eta_i^k\middle|\boldsymbol{\theta}=\theta\right)\\ &= \Pr\left(a_i+\boldsymbol{n}_i>\eta_i^k\middle|\boldsymbol{\theta}=\theta\right)\\ &= 1-\Phi\left(\frac{\eta_i^k-a_i}{\sigma}\right). \end{aligned} \quad (15)$$

Substituting (14), (15) and $d_{\min}^k = 2N_k/L$ into (13), we have

$$P_{\mathrm{e}}^k \leq \sum_{\ell=1}^{L}\int_{\mathcal{R}_\ell^k}\left\{\sum_{j=1,\,j\neq\ell}^{L}\left(1-\frac{\left(\sum_{i\in S_\ell^k}\Phi\left(\frac{\eta_i^k-a_i}{\sigma}\right)-\sum_{i\in S_j^k}\Phi\left(\frac{\eta_i^k-a_i}{\sigma}\right)\right)^2}{N_k^2/L^2}\right)^{N_k/L}\right\}dF^k(\theta), \quad (16)$$

[5]Lemma 2 in [34] literally states that if $\lambda_{\ell,j}^k<0$, then

$$\Pr\left(\sum_{i\in\mathcal{S}_\ell^k\bigcup S_j^k}\boldsymbol{z}_{i,\ell}^k\geq 0\middle|\boldsymbol{\theta}=\theta\right)\leq\left[1-(\lambda_{\ell,j}^k)^2\right]^{d_{\min}^k/2}. \quad (12)$$

Since (12) remains valid when $\lambda_{\ell,j}^k=0$, we relax the condition in (11) by adopting $\lambda_{\ell,j}^k\leq 0$.

provided that[6] for $\theta\in\mathcal{R}_\ell^k$ and every $j\neq\ell$,

$$\sum_{i\in S_\ell^k}\Phi\left(\frac{\eta_i^k-a_i}{\sigma}\right)\leq\sum_{i\in S_j^k}\Phi\left(\frac{\eta_i^k-a_i}{\sigma}\right). \quad (17)$$

Our goal is to find η_i^k for each $i\in\mathcal{S}^k$ that minimizes the right-hand-side of (16) subject to the constraints in (17).

In order to simplify the optimization of (16), we utilize two assumptions.

Assumption 1 (Homomorphic sensor deployment): There exists a bijection mapping $\beta=\beta_{\ell,j}^k:\mathcal{S}_\ell^k\mapsto\mathcal{S}_j^k$ such that for every $\theta\in\mathcal{R}_\ell^k$, one can find $\tilde{\theta}\in\mathcal{R}_j^k$ that satisfies $d_{\mathrm{E}}(\theta,\theta_i)=d_{\mathrm{E}}(\tilde{\theta},\theta_{\beta(i)})$ for all $i\in\mathcal{S}_\ell^k$.[7]

Assumption 2 (Non-decreasing distances after mapping): The bijective mapping given in Assumption 1 also satisfies that $d_{\mathrm{E}}(\theta,\theta_i)\leq d_{\mathrm{E}}(\theta,\theta_{\beta(i)})$ for every $i\in\mathcal{S}_\ell^k$ and $\theta\in\mathcal{R}_\ell^k$.

In Figure 2, we illustrate a set of bijection mappings that validate Assumption 1. In this figure, there are four sensors in each super-region. The sensors with the same color establish the required $\binom{4}{2}=6$ bijection mappings between super-regions $\mathcal{R}_1^k$, $\mathcal{R}_2^k$, $\mathcal{R}_3^k$ and $\mathcal{R}_4^k$. The existences of $\tilde{\theta}$ respectively in super-regions $\mathcal{R}_2^k$, $\mathcal{R}_3^k$ and $\mathcal{R}_4^k$, which satisfies $d_{\mathrm{E}}(\theta,\theta_i)=d_{\mathrm{E}}(\tilde{\theta},\theta_{\beta(i)})$ for all $i\in\mathcal{S}_1^k$ and a given θ, is demonstrated in Figure 2(b), where the pair of equal distance $d_{\mathrm{E}}(\theta,\theta_i)$ and $d_{\mathrm{E}}(\tilde{\theta},\theta_{\beta(i)})$ is depicted in the same color.

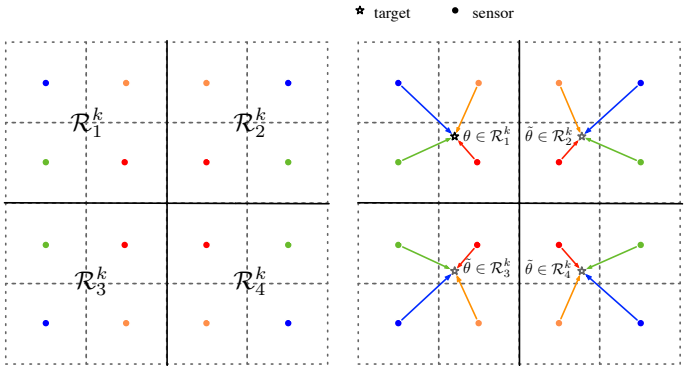


Fig. 2. Illustration of the homomorphic sensor deployment in Assumption 1. Sensors with the same color form the required bijection mappings between super-regions $\mathcal{R}_1^k$, $\mathcal{R}_2^k$, $\mathcal{R}_3^k$ and $\mathcal{R}_4^k$. The existence of $\tilde{\theta}$, whose distance to the mapped sensor $\beta(i)$ is equal to the distance between a given θ to the sensor i before bijection mapping, is demonstrated in (b).

Assumption 2 dictates that the distance between a target and a sensor in the same super-region is never greater than that between

[6]By Eqs. (14) and (15), we can equivalently re-write (17) as either

$$\sum_{i\in S_\ell^k}\Pr\left(\boldsymbol{s}_i>\eta_i^k\middle|\boldsymbol{\theta}=\theta\right)\geq\sum_{i\in S_j^k}\Pr\left(\boldsymbol{s}_i>\eta_i^k\middle|\boldsymbol{\theta}=\theta\right)$$

or

$$\sum_{i\in S_\ell^k}\Pr\left(\boldsymbol{u}_i^k=c_{\ell,i}^k\middle|\boldsymbol{\theta}=\theta\right)\geq\sum_{i\in S_j^k}\Pr\left(\boldsymbol{u}_i^k=c_{\ell,i}^k\middle|\boldsymbol{\theta}=\theta\right).$$

Thus under the assumption that $\theta\in\mathcal{R}_\ell^k$, constraint (16) implies that in comparison with the RSS received by sensors in $\mathcal{R}_j^k$, the RSS experienced by sensors in $\mathcal{R}_\ell^k$ tends to be larger with a higher sum probability since the target $\theta\in\mathcal{R}_\ell^k$ is supposed to be statistically nearer to those sensors in the same super-region $\mathcal{R}_\ell^k$.

[7]We drop parameters ℓ, j and k in the notation of mapping β to simplify its representation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

the same target and any mapped sensor in another super-region. For an easy understanding, two cases concerned by Assumption 2 are illustrated in Figure 3, where the length of the solid line is obviously no larger than that of any dashed line.

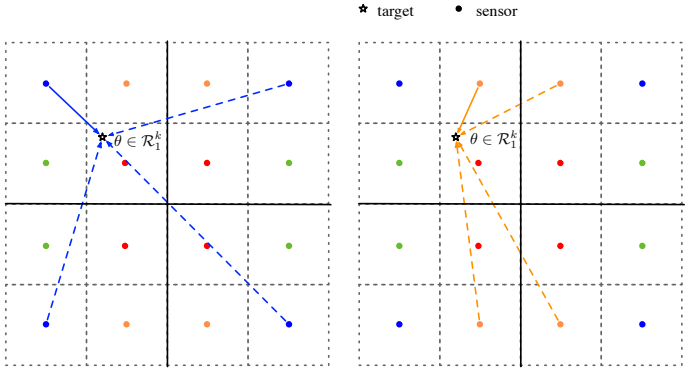


Fig. 3. Illustration of Non-decreasing distances after mapping in Assumption 2

It can be straightforwardly verified that these two assumptions can be satisfied if the $\beta(i)$th sensor in super-region $\mathcal{R}_j^k$ is the mirror point of the ith sensor at super-region $\mathcal{R}_\ell^k$ with respect to the middle reflection line between $\mathcal{R}_j^k$ and $\mathcal{R}_\ell^k$. It then immediately follows from Assumption 2 that $a_i = \sqrt{P_0}/d_{\mathrm{E}}(\theta,\theta_i) \geq a_{\beta(i)} = \sqrt{P_0}/d_{\mathrm{E}}(\theta,\theta_{\beta(i)})$ for every $i \in \mathcal{S}_\ell^k$ and $\theta \in \mathcal{R}_\ell^k$. Hence, if we set $\eta_i^k = \eta_{\beta(i)}^k$ for $i \in \mathcal{S}_\ell^k$, then constraint (17) is valid, i.e.,

$$\begin{aligned}
&\eta_i^k - a_i \leq \eta_{\beta(i)}^k - a_{\beta(i)} \ \forall\ i \in \mathcal{S}_\ell^k \\
&\Leftrightarrow \Phi\left(\frac{\eta_i^k - a_i}{\sigma}\right) \leq \Phi\left(\frac{\eta_{\beta(i)}^k - a_{\beta(i)}}{\sigma}\right) \ \forall\ i \in \mathcal{S}_\ell^k \\
&\Rightarrow \sum_{i\in S_\ell^k} \Phi\left(\frac{\eta_i^k - a_i}{\sigma}\right) \\
&\leq \sum_{i\in S_\ell^k} \Phi\left(\frac{\eta_{\beta(i)}^k - a_{\beta(i)}}{\sigma}\right) = \sum_{i\in S_j^k} \Phi\left(\frac{\eta_i^k - a_i}{\sigma}\right). \qquad (18)
\end{aligned}$$

As a result of the two assumptions, together with uniform $F^k(\theta)$, we end up with the following objective function for the optimization of $\{\eta_i^k\}_{i\in\mathcal{S}_1^k}$:

$$\begin{aligned}
P_{\mathrm{e}}^k &\leq \sum_{\ell=1}^{L} \int_{\mathcal{R}_\ell^k} \left\{ \sum_{j=1,\, j\neq\ell}^{L} \left(1 \right.\right. \\
&\left.\left. - \frac{\left(\sum_{i\in S_\ell^k} \Phi\left(\frac{\eta_i^k - a_i}{\sigma}\right) - \sum_{i\in S_j^k} \Phi\left(\frac{\eta_i^k - a_i}{\sigma}\right)\right)^2}{N_k^2/L^2} \right)^{N_k/L} \right\} dF^k(\theta), \\
&= \frac{1}{|\mathcal{R}^k|} \sum_{\ell=1}^{L} \int_{\mathcal{R}_\ell^k} \sum_{j=1,\, j\neq\ell}^{L} \left(1 \right. \\
&\left. - \frac{\left(\sum_{i\in S_\ell^k} \left[\Phi\left(\frac{\eta_i^k - a_i}{\sigma}\right) - \Phi\left(\frac{\eta_i^k - a_{\beta(i)}}{\sigma}\right)\right]\right)^2}{N_k^2/L^2} \right)^{N_k/L} d\theta,
\end{aligned}$$

where $|\mathcal{R}^k|$ denotes the area of $\mathcal{R}^k$. We summarize the derivation in this section in the next Proposition.

Proposition 1: Given that a set of bijection mapping $\beta = \beta_{\ell,j}^k : \mathcal{S}_\ell^k \mapsto \mathcal{S}_j^k$ satisfies Assumptions 1 and 2 for $1 \leq k \leq k_{\text{stop}}$ and $1 \leq \ell, j \leq L$, and subject to that all the previous $(k-1)$ iterations succeed to identify the correct super-region that the target is located in, the misclassification probability of the kth iteration is upper-bounded by

$$\begin{aligned}
P_{\mathrm{e}}^k \leq \frac{L}{|\mathcal{R}^k|} \int_{\mathcal{R}_1^k} \sum_{j=2}^{L} \left(1 \right. \\
\left. - \frac{\left(\sum_{i\in S_1^k} \left[\Phi\left(\frac{\eta_i^k - a_i}{\sigma}\right) - \Phi\left(\frac{\eta_i^k - a_{\beta(i)}}{\sigma}\right)\right]\right)^2}{N^2/L^{2k}} \right)^{N/L^k} d\theta,
\end{aligned}$$

where $\{\eta_i\}_{i\in\mathcal{S}^k}$ are a set of pre-specified local thresholds for sensors in $\mathcal{R}^k$ that uphold $\eta_{\beta(i)} = \eta_i$ for every $i \in \mathcal{S}^k$, and $a_i = a_i(\theta) = \sqrt{P_0}/d_{\mathrm{E}}(\theta,\theta_i)$ is the noise-free signal received by the ith sensor, provided that θ is uniformly distributed over the ROI $\mathcal{R}^k$, and

$$\begin{aligned}
\Omega^k \triangleq \int_{\mathcal{R}_\ell^k} \sum_{j=1,\, j\neq\ell}^{L} \left(1 \right. \\
\left. - \frac{\left(\sum_{i\in S_\ell^k} \left[\Phi\left(\frac{\eta_i^k - a_i}{\sigma}\right) - \Phi\left(\frac{\eta_i^k - a_{\beta(i)}}{\sigma}\right)\right]\right)^2}{N^2/L^{2k}} \right)^{N/L^k} d\theta \qquad (19)
\end{aligned}$$

is the same for $1 \leq \ell \leq L$.

We close this section by remarking that it might be possible to determine a set of local thresholds $\{\eta_i^k\}_{1\leq i\leq N_k}$ without the two assumptions but to resort only to constraint (17). However, the numerical challenge, as required to examine the validity of (17) for every choice of candidate thresholds as well as the calculation of (16), may make the task of searching for the best thresholds computationally intractable. This brings up the value of the two assumptions in Proposition 1, which not only reduces the number of thresholds to be determined from N_k down to N_k/L, but makes possible the simplification of the double summations indexed by ℓ and j in (16) down to one summation indexed by j, thereby greatly weakening the previously mentioned numerical challenge. Since the particular mirror-based homomorphic sensor deployment structure is physically realizable, Proposition 1 can be well applied to practical WSNs with a finite number of sensors.

VI. Local Threshold Design

In this section, we develop an algorithmic procedure to determine the thresholds $\{\eta_i^k\}_{i\in\mathcal{S}_1^k}$ by minimizing Ω^k given in Proposition 1. Since the exact evaluation of Ω^k requires a closed-form integration from

$$a_i = a_i(\theta) = \sqrt{P_0}/d_{\mathrm{E}}(\theta,\theta_i),$$

which is actually analytically intractable, we maximize an approximate quantity by Monte Carlo integration instead:

$$\begin{aligned}
\Gamma^k \triangleq \frac{1}{|\mathcal{T}_1^k|} \sum_{\theta\in\mathcal{T}_1^k} \sum_{j=2}^{L} \left(1 \right. \\
\left. - \frac{\left(\sum_{i\in S_1^k} \left[\Phi\left(\frac{\eta_i^k - a_i}{\sigma}\right) - \Phi\left(\frac{\eta_i^k - a_{\beta(i)}}{\sigma}\right)\right]\right)^2}{N_k^2/L^2} \right)^{N_k/L}, \qquad (20)
\end{aligned}$$

where $\mathcal{T}_1^k$ is a set consisting of a finite number of typical discrete points in $\mathcal{R}_1^k$ and $|\mathcal{T}_1^k|$ indicates the number of points in $\mathcal{T}_1^k$. It is reasonable to assume that as long as the number of points in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

$\mathcal{T}_1^k$ is adequately large and they are evenly distributed over $\mathcal{R}_1^k$, minimization of the criterion Γ^k should yield near-optimal thresholds, where by optimality, we mean the thresholds that minimize Ω^k.

From (1) and (2), the binary value of $\boldsymbol{u}_i^k$ is determined by

$$\boldsymbol{s}_i = \sqrt{P_0}\,\frac{d_0}{\boldsymbol{d}_i} + \boldsymbol{n}_i \underset{\boldsymbol{u}_i^k=0}{\overset{\boldsymbol{u}_i^k=1}{\gtrless}} \eta_i^k,$$

which under $d_0 = 1$ and $\boldsymbol{n}_i = 0$, is equivalent to

$$\boldsymbol{d}_i \underset{\boldsymbol{u}_i^k=0}{\overset{\boldsymbol{u}_i^k=1}{\lessgtr}} \frac{\sqrt{P_0}}{\eta_i^k}.$$

Since $\boldsymbol{d}_i = d_{\mathrm{E}}(\boldsymbol{\theta}, \theta_i)$ is the Euclidean distance between the target and the ith sensor, it is reasonable to infer that the reciprocal of the optimal threshold, i.e., $1/\eta_i^{k*}$, will not be larger than $A_i^k/\sqrt{P_0}$, where $A_i^k \triangleq \max_{\theta\in\mathcal{R}^k} d_{\mathrm{E}}(\theta, \theta_i)$ is the distance between the ith sensor and the farthest boundary point of the ROI $\mathcal{R}^k$ to it. In addition, since $\boldsymbol{d}_i$ is nonnegative, a negative η_i^k will not be optimal. This suggests a search space of $\sqrt{P_0}/\eta_i^k$ between 0 and A_i^k.

In order to conduct a computationally efficient search that yields an accurate solution, we fix the step size Δ to be $1/8$ of the minimum distance between the sensors, and partition the interval of $(0, A_k^i]$ into $Q_i^k \triangleq \lfloor A_k^i/\Delta \rfloor$ sub-intervals of length Δ and one sub-interval of length $A_k^i - Q_i^k\Delta$. We then examine Γ^k based on $\sqrt{P_0}/\eta_i^k$ being the end points of these sub-intervals, i.e., $\sqrt{P_0}/\eta_i^k \in \{\Delta, 2\Delta, 3\Delta, \ldots, Q_i^k\Delta\}$. Under such setting, the values of η_i^k under test are confined in $\left\{\frac{\sqrt{P_0}}{Q_i^k\Delta}, \frac{\sqrt{P_0}}{(Q_i^k-1)\Delta}, \frac{\sqrt{P_0}}{(Q_i^k-2)\Delta}, \ldots, \frac{\sqrt{P_0}}{\Delta}\right\}$. Notably, we intentionally make the setting of Q_i^k to be independent of the choice of P_0 to facilitate our simulations for different radiating signal-to-noise power ratio $\gamma_{rad} \triangleq P_0/\sigma^2$. With an adequately small Δ, the optimal threshold η_i^{k*} can be approached. Our experiments indicate that the optimal threshold η_i^{k*} is always markedly larger than $\sqrt{P_0}/(Q_i^k\Delta)$ and is never near the largest possible value $\sqrt{P_0}/\Delta$ under test.

It should be noted that the optimal local thresholds of the sensors can be determined before their deployment in the field. Hence the complexity of searching for the best local thresholds will never add the operational complexity of the sensors or the FC.

VII. Experimental Results

In this section, we present the simulation results that show the significant improvement of system performance when the proposed local threshold design is employed.

The system setting of our experiments is described as follows. The sensors are deployed in a square grid, and the minimum pair-wise distance among sensors is 1. For the computation of Γ in (20), we set $P_0 = 200$ and $\sigma = 3$ so that the radiating signal-to-noise power ratio $\gamma_{rad} \triangleq P_0/\sigma^2 = 13.5$ dB. For all the simulations, independent fading channels between the sensors and the FC were employed. While the performance of only the hard-decision decoding scheme is shown in Figures 4 to 7, the performances of both hard-decision decoding and soft-decision decoding schemes are presented in Figures 8 to 11. For each simulation, 5000 target locations are randomly generated for the numerical evaluation of the performance.

Under the setting that the designated area $\mathcal{R}$ is partitioned into 4 regions, each of which consists of 16 sensors, Table I gives the optimal local thresholds $\{\eta_i^*\}_{i=1}^{64}$ obtained by using a numerical search method that is frequently employed for system optimization, often referred to as the person-by-person optimization procedure [35]. One can observe from Table I that the values of the local thresholds, marked in red, are relatively large. It reveals the fact that the sensors located near the border between regions require a higher local threshold in order to reduce the chance of false alarm of incorrectly claiming that a target was within the region that the sensor belongs to. It coincides with the theoretical implication that the sensors located near the borders among regions would tend to make wrong local decisions with higher probabilities. Hence, the results of Table I are justified. Later, we employ the local thresholds from Table I to show their effectiveness with two performance metrics, which are the detection probability of the region that the target is located in, and the MSE of the average distance between the true target location and its estimate.

TABLE I
Optimal local thresholds $\{\eta_i^*\}_{i=1}^{64}$ under the setting that the designated area $\mathcal{R}$ is partitioned into $M = 4$ regions, each of which consists of 16 sensors. Here, we assume that the power measured at the reference distance $d_0 = 1$ is $P_0 = 200$ and the variance of the sensing noise is $\sigma^2 = 9$.

$\mathcal{R}_3$				$\mathcal{R}_4$			
4.714	7.071	6.285	8.703	8.703	6.285	7.071	4.714
6.655	5.955	6.655	6.655	6.655	6.655	5.955	6.655
6.285	7.071	7.071	8.081	8.081	7.071	7.071	6.285
5.955	7.542	10.285	16.162	16.162	10.285	7.542	5.955
5.955	7.542	10.285	16.162	16.162	10.285	7.542	5.955
6.285	7.071	7.071	8.081	8.081	7.071	7.071	6.285
6.655	5.955	6.655	6.655	6.655	6.655	5.955	6.655
4.714	7.071	6.285	8.703	8.703	6.285	7.071	4.714
$\mathcal{R}_1$				$\mathcal{R}_2$			

TABLE II
The resultant probability bounds Γ in (20) as a function of total number of sensors N, where the designated area $\mathcal{R}$ is partitioned into $M = 4$ regions

N	N/M	Γ
64	16	0.2256
256	64	0.0319
1024	256	0.0032

As a reference, we list in Table II the probability bounds Γ computed using the thresholds obtained from the proposed method. We can observe that by quadrupling the number of sensors in an ROI of the same size, we can, in the sense of upper bounds, reduce the probability of misclassification by one order of magnitude.

A major advantage of the DCFECC scheme is its capability to compensate for adversarial action from Byzantine sensors without the need to identify them [1]. This is in principle similar to the error correcting capability of a channel code. To show this aspect, we compare the probabilities of detection (i.e., $P_{\mathrm{d}} = 1 - P_{\mathrm{e}}$) based on thresholds adopted in [1] with those obtained using the proposed method in the presence of Byzantine adversaries, and summarize the results in Figure 4. It should be noted that in our simulations, a Byzantine sensor is assumed to maliciously flip its local decision (i.e., $\boldsymbol{u}_i$) before sending it to the FC in order to alter the global inference of the true hypothesis. The Byzantine sensors are randomly chosen among all the sensors in our simulations. Our experimental results indicate that an improvement in the probability of detection can be obtained by adopting the proposed thresholds. As an example, when the fraction of Byzantine sensors is equal to 25%, the probability of detection increases from 0.55 to 0.75 after replacing the thresholds used in [1] by the ones obtained by using the proposed method. We also test whether different ordering of thresholds during the numerical person-by-person search affects the performance of the resulting thresholds in Figure 4 and found that the ordering of thresholds during the numerical search indeed has little impact on the probability of detection as well as the resultant threshold values.

Another common performance index for target localization is the MSE of the average distance between the true target position and its estimate. In this paper, the estimated target location is set to be the center of the region that the target is declared to lie in. This definition is the same as the one used in [1]. Figure 5 shows that when the fraction of Byzantine sensors is 25%, the MSE of the average distance between the true target position and its estimate is 2.7 if the thresholds in [1] are used, while it is reduced to 2.2 if the proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

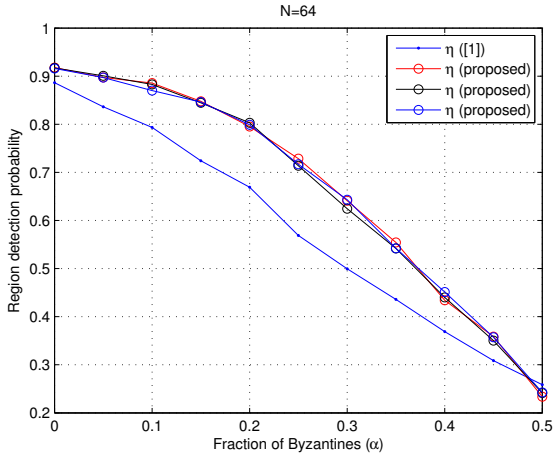


Fig. 4. Probabilities of detection resulting from thresholds employed in [1] and from those derived from the proposed method with three different orderings of thresholds during the numerical person-by-person search

thresholds are used instead. As a result, 18.5% improvement in the accuracy of target positioning can be achieved on an average. Also shown in Figure 5 is that different ordering of thresholds during the numerical search yields almost identical MSEs. This coincides with what we have observed from Figure 4.

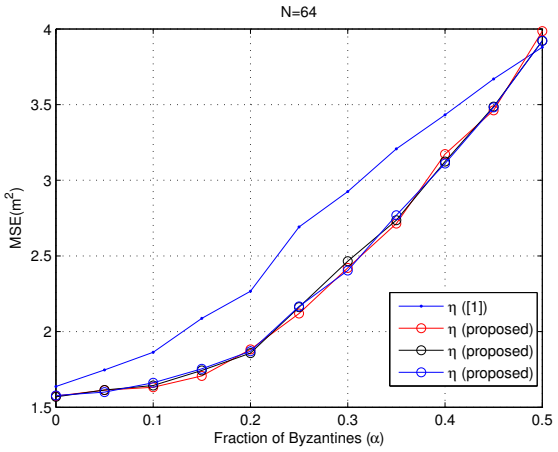


Fig. 5. MSEs of the average distance between the true target position and the center of the declared region determined based on thresholds used in [1] and also based on those derived from the proposed method with three different orderings of thresholds during the numerical person-by-person search

Next, we examine the performance of the optimized thresholds acquired by using the proposed method in situations when iterative classification is employed. For $L = 4$, we set the number of sensors at the first, second and third iterations to be $N_1 = 1024$, $N_2 = 256$ and $N_3 = 64$, respectively. At the final iteration, the region that the target is declared to lie in will contain only $N_3/L = 16$ sensors. The experimental results are illustrated in Figures 6 and 7. We observe from Figure 6 that when the number of Byzantine sensors reaches 25% of the total number of sensors at each iteration, the probability of detection for the optimized thresholds reaches 0.68 but that for the thresholds used in [1] is only 0.40.

In Figure 7, we observe that at the end of the first iteration, the thresholds in [1] and the thresholds from the proposed method, although seemingly different, yield almost the same MSEs when the fraction of Byzantine sensors is below 25%. It is during the following iterations that the optimized thresholds from the proposed method start to outperform the thresholds used in [1]. More specifically, when iterative classification is employed on the three-layer DCFECC system we consider here and 25% of sensors are experiencing Byzantine attacks, the MSE of the average distance between the target location and its estimate is 1.0 if the thresholds in [1] are used, while it is reduced to 0.7 if the optimized thresholds from the proposed method are adopted instead. As a result, 30% improvement in the accuracy of target positioning can be achieved on an average.

In addition, Figure 7 illustrates how iterative classification on the three-layer DCFECC system improves over iterations in MSE performance index. More specifically, when 25% of the sensors experience Byzantine attacks and the sensors employ the optimized thresholds from the proposed method, the MSE performance is improved from 1.5 down to 0.7 when iterative classification migrates from the first iteration to the third iteration. Over 50% improvement in the accuracy of target positioning is obtained.

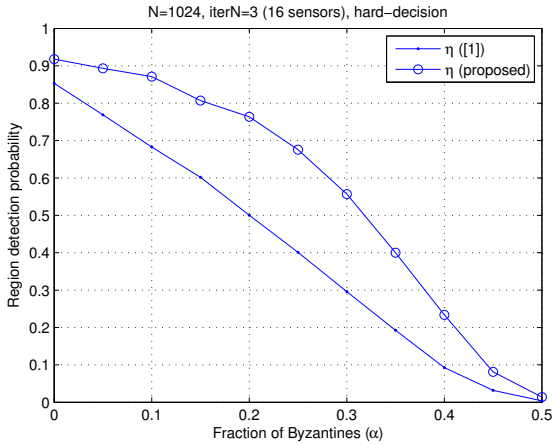


Fig. 6. Probabilities of detection for thresholds in [1] and for those obtained from the proposed method under iterative classification

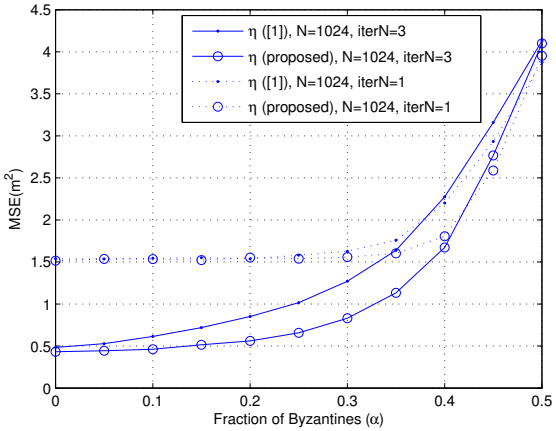


Fig. 7. MSEs between the true target position and the center of the declared region for thresholds used in [1] and for those obtained from the proposed method under iterative classification

Furthermore, we investigate the performance of the proposed local threshold design when the system operates at different signal-to-noise ratios $\gamma_w \triangleq E_b/\sigma_w^2$ for the wireless links defined in (4). The results are summarized in Figures 8 and 9, where two fractions of Byzantine sensors are tested, namely, $\alpha = 0$ and $\alpha = 25\%$. Both hard-decision based classification, which performs the minimum Hamming distance fusion based on binary quantized received signals in (4), and soft-decision based classification, which determines the target region by searching the rows of $\mathbb{C}$ that is closest to the received signals in Euclidean distance as in (7), are examined. Several observations can be made on these two figures. First, soft-decision based classification always performs better than hard-decision based classification for the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

same system setting. This observation is applicable to both Figures 8 and 9. The performance gap between hard and soft-decision based classification methods, however, vanishes when $\gamma_{\rm w}$ is beyond -2 dB. Secondly, when the fraction of Byzantine sensors is $\alpha = 25\%$, the optimized thresholds from the proposed method improve the system performance considerably over the thresholds in [1]. This is in contrast to the limited performance improvement due to the adoption of the optimized thresholds from the proposed method instead of those used in [1] when no Byzantine sensors are present. Thirdly, the performances of all system settings saturate when $\gamma_{\rm w}$ is greater than -4 dB because Byzantine attacks and wireless channel fading begin to dominate the deterioration of the data bits received at the FC. Last, hard-decision based classification that employs the optimized thresholds from the proposed method beats soft-decision based classification that employs the thresholds obtained from [1] in almost all the cases considered in the two figures except for $\alpha = 0$ and $\gamma_{\rm w} \leq -6$ dB. This confirms the superiority of our new threshold design over the one in [1].

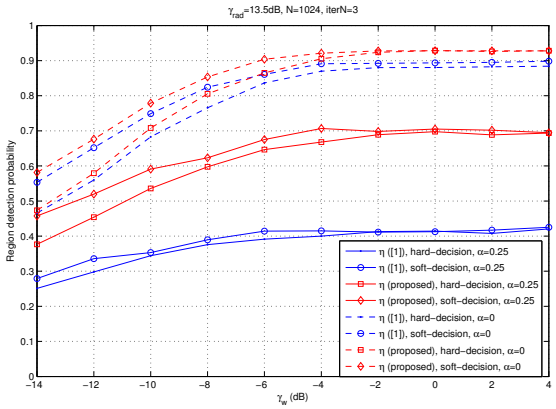


Fig. 8. Probabilities of detection for thresholds used in [1] and for those obtained from the proposed method under iterative classification and fading wireless links

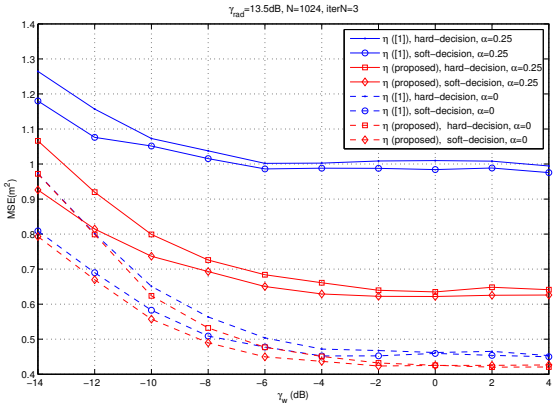


Fig. 9. MSEs between the true target position and the center of the declared region for thresholds used in [1] and for those obtained from the proposed method under iterative classification and fading wireless links

In all the above threshold designs, we assumed $P_0 = 200$ and $\sigma = 3$, resulting in a radiating signal-to-noise ratio $\gamma_{rad} = P_0/\sigma^2 = 13.5$ dB. A natural question that follows is whether the optimized thresholds obtained at $\gamma_{rad} = 13.5$ dB are robust in performance for other γ_{rad} values. Figures 10 and 11 address this point. Fixing $\gamma_{\rm w} = -4$ dB to have a saturated performance, we observe from the two figures that when γ_{rad} is larger than 6 dB, the optimized thresholds designed based on $\gamma_{rad} = 13.5$ dB have little degradation and still markedly outperform the thresholds in [1]. The superiority of the optimized thresholds from the proposed method over those in [1], however, gradually diminishes when γ_{rad} moves away from the 13.5 dB value that was assumed at the design stage. By noting that the radiating signal-to-noise ratio sensed by the ith sensor γ_i is equal to

$$\gamma_i \text{ (dB)} = \gamma_{rad} \text{ (dB)} - 20\log_{10}(d_i/d_0),$$

it may be realistic to require that the nearby nine sensors around the target in a square grid of size 2×2 have all their γ_i's larger than 0 dB; hence, by assuming d_i to be the length of the side of the 2×2 square grid, which is $2 \cdot d_0$ in our setting, it is justified to place our attention on those $\gamma_{rad} \geq 20\log_{10}(2) = 6$ dB.

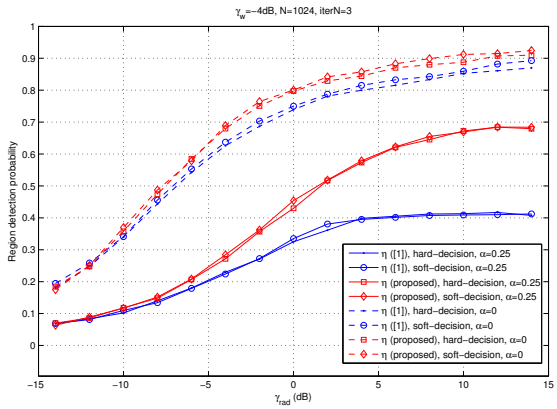


Fig. 10. Probabilities of detection as a function of the radiating signal-to-noise ratio for thresholds used in [1] and for those obtained from the proposed method under iterative classification and fading wireless links

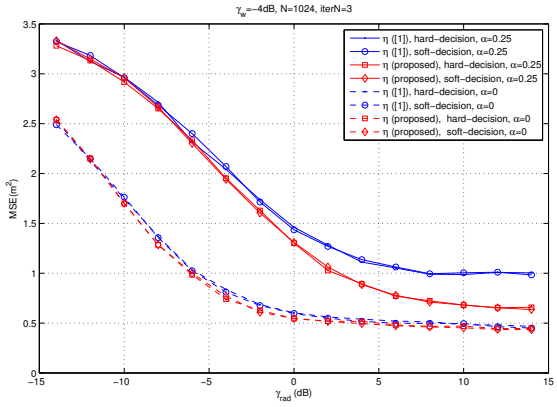


Fig. 11. MSEs between the true target position and the center of the declared region, as a function of the radiating signal-to-noise ratio, for thresholds used in [1] and for those obtained from the proposed method under iterative classification and fading wireless links

VIII. Conclusion

A highly innovative approach for target localization via iterative classification and the use of error control codes was presented in [1]. It was shown to be quite robust and to provide high accuracy even in the presence of sensor failures and communication errors when the number of sensors grows without bound. The issue of optimal threshold design at local sensors, however, was not addressed in [1], particularly when the number of sensors is fixed and finite. This paper considered threshold design for the problem formulation in [1] for a practical WSN of finite size and thus completes the work started in [1] by making it applicable in practice.

With this objective, in this paper, a systematic procedure to find the set of optimized RSS thresholds for iterative classification over a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

multi-layer hierarchical DCFECC system of [1] was proposed. The key to the effectiveness in performance of the newly found RSS thresholds is the establishment of a theoretical upper bound on the probability of misclassification, which we afterwards adopted as the objective function in threshold search.

In simulation experiments, we took into account all the imperfections over WSNs, including sensing noise, fast fading wireless links and Byzantine attacks. Our simulation results demonstrated the necessity of an optimized threshold design for improvement of both probability of detection and MSEs, in particular in the situation where a moderately large fraction of sensors are Byzantines. Performances of both hard-decision and soft-decision based classifications were evaluated. We observed, however, that hard-decision based classification may outperform soft-decision based one if the former employs a better set of RSS thresholds. This further substantiates the significance of the proposed RSS threshold design in a multi-layer hierarchical DCFECC system of finite size.

The estimated target location in this work is taken to be the center of the final ROI region obtained from iterative classification. Further improvement could be possible by incorporating other estimation approaches with the tradeoff that multiple-bit transmissions may be necessary. For example, a scheme can utilize the RSS of the beacon signals received by the sensors in the final ROI to produce a better estimate of the target position instead of simply using the region center as the final estimate. Carrying the RSS information from sensors to the FC, however, requires definitely more transmission effort. Alternatively, to replace the static way the super-regions are divided with a dynamic one through iterations (in order to avoid the ambiguity introduced when the target happens to be near the boundary of two divisions) may also benefit the estimation accuracy. As such, a dynamic network management mechanism at the FC with certain communication feedbacks to sensors may be necessary as sensors should be notified about the new dynamic divisions they belong to at the next iteration. It would be interesting to examine the tradeoff among energy consumption, management cost and the improvement of the estimate for the proposed iterative classification under the above modifications, in particular in a fading environment with possible Byzantine attacks.

Like many other works on localization [7], [8], [9] that are based on received signal strengths, the current work considered a one-shot location estimation for the localization of a single target. Due to the robustness of the proposed hierarchical DCFECC system that was shown to be capable of simultaneously compensating for sensing noise, imperfection of wireless links and Byzantine attacks without the need to identify the cause of information deterioration, its extension to motion tracking that faces inevitably varying noise and link statistics could be an interesting problem to further explore. A challenging future work that may be of importance and usefulness is to investigate whether a set of quality RSS thresholds can be determined analytically from the probability bound. By this, useful rules of thumb on quality RSS threshold design could be introduced into the target localization literature.

REFERENCES

[1] A. Vempaty, Y. S. Han, and P. K. Varshney, "Target localization in wireless sensor networks using error correcting codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 1, pp. 697–712, Jan. 2014.

[2] R. Peng and M. Sichitiu, "Angle of arrival localization for wireless sensor networks," in *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks. (SECON'06).*, vol. 1, Sept. 2006, pp. 374–382.

[3] E. Xu, Z. Ding, and S. Dasgupta, "Wireless source localization based on time of arrival measurement," in *2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, Mar. 2010, pp. 2842–2845.

[4] N. Patwari, A. O. Hero, M. Perkins, N. S. Correal, and R. J. O'Dea, "Relative location estimation in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 51, no. 8, pp. 2137–2148, Aug. 2003.

[5] K. W. Cheung, H. C. So, W. K. Ma, and Y. T. Chan, "Least squares algorithms for time-of-arrival-based mobile location," *IEEE Trans. Signal Process.*, vol. 52, no. 4, pp. 1121–1130, Apr. 2004.

[6] K. Yang, J. An, X. Bu, and G. Sun, "Constrained total least-squares location algorithm using time-difference-of-arrival measurements," *IEEE Trans. Vehicular Technology*, vol. 59, no. 3, pp. 1558–1562, Mar. 2010.

[7] D. Li, K. D. Wong, Y. H. Hu, and A. M. Sayeed, "Detection, classification, and tracking of targets," *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 17–29, Mar. 2002.

[8] D. Li and Y. H. Hu, "Energy-based collaborative source localization using acoustic microsensor array," *EURASIP Journal on Applied Signal Processing*, vol. 2003, pp. 321–337, Jan. 2003.

[9] T. L. T. Nguyen, F. Septier, H. Rajaona, G. W. Peters, I. Nevat, and Y. Delignon, "A Bayesian perspective on multiple source localization in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 64, no. 7, pp. 1684–1699, Apr. 2016.

[10] R. Niu and P. K. Varshney, "Target location estimation in sensor networks with quantized data," *IEEE Trans. Signal Process.*, vol. 54, no. 12, pp. 4519–4528, Dec. 2006.

[11] D. Li and Y. H. Hu, "Energy-based collaborative source localization using acoustic microsensor array," *EURASIP Journal on Applied Signal Processing*, vol. 2003, no. 4, pp. 321–337, 2003.

[12] X. Sheng and Y. H. Hu, "Maximum likelihood multiple-source localization using acoustic energy measurements with wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 53, no. 1, pp. 44–53, Jan. 2005.

[13] Z. Yang and L. Tong, "Cooperative sensor networks with misinformed nodes," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4118–4133, Dec. 2005.

[14] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attacks," *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 16–29, Jan. 2009.

[15] A. Vempaty, L. Tong, and P. K. Varshney, "Distributed inference with Byzantine data: State-of-the-art review on data falsification attacks," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 65–75, Sept. 2013.

[16] A. Vempaty, O. Ozdemir, K. Agrawal, H. Chen, and P. K. Varshney, "Localization in wireless sensor networks: Byzantines and mitigation techniques," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1495–1508, Mar. 2013.

[17] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, Inc., 2004.

[18] T.-Y. Wang, Y. S. Han, P. K. Varshney, and P.-N. Chen, "Distributed fault-tolerant classification in wireless sensor networks," *IEEE J Sel. Areas Comm.*, vol. 23, no. 4, pp. 724–734, Apr. 2005.

[19] A. Vempaty, Y. S. Han, and P. K. Varshney., "Target localization in wireless sensor networks using error correcting codes in the presence of Byzantines," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP 2001)*, Vancouver, Canada, May 2013, pp. 5195–5199.

[20] ——, "Byzantine tolerant target localization in wireless sensor networks over non-ideal channels," in *Proc. 13th Int. Symp. Commun. Inf. Technologies (ISCIT 2013)*, Samui Island, Thailand, Sept. 2013.

[21] M. P. Michaelides and C. G. Panayiotou, "SNAP: Fault tolerant event location estimation in sensor networks using binary data," *IEEE Trans. Computers*, vol. 58, no. 9, pp. 1185–1197, Sept. 2009.

[22] M. P. Michaelides, C. Laoudias, and C. G. Panayiotou, "Fault tolerant localization and tracking of multiple sources in wsns using binary data," *IEEE Trans. Mobile Computing*, vol. 13, no. 6, pp. 1213–1227, Jun. 2014.

[23] M. R. Islam, "Error correction codes in wireless sensor network: An energy aware approach," *International Journal of Computer & Information Engineering*, vol. 4, no. 1, pp. 59–64, Jan. 2010.

[24] S. Marano, V. Matta, P. Willett, and L. Tong, "DOA estimation via a network of dumb sensors under the SENMA paradigm," *IEEE Signal Processing Letters*, vol. 12, no. 10, pp. 709–712, Oct. 2005.

[25] ——, "Support-based and ML approaches to DOA estimation in a dumb sensor network," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1563–1567, Apr. 2006.

[26] M. Guerriero, S. Marano, V. Matta, and P. Willett, "Some aspects of DOA estimation using a network of blind sensors," *Signal Process.*, vol. 88, no. 11, pp. 2640–2650, Nov. 2008.

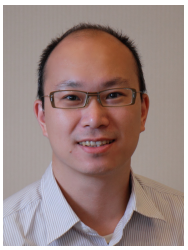
[27] O. Kosut and L. Tong, "Distributed source coding in the presence of Byzantine sensors," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2550–2565, Jun. 2008.

[28] T. Snow, C. Fulton, and W. J. Chappell, "Transmit-receive duplexing using digital beamforming system to cancel self-interference," *IEEE Trans. Microwave Theory and Techniques*, vol. 59, no. 12, pp. 3494–3503, Dec. 2011.

[29] J. f. Chamberland and V. V. Veeravalli, "Wireless sensors in distributed detection applications," *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 16–25, May 2007.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2670531, IEEE Transactions on Information Forensics and Security

[30] O. P. Kreidl and A. S. Willsky, "An efficient message-passing algorithm for optimizing decentralized detection networks," *IEEE Trans. Automatic Control*, vol. 55, no. 3, pp. 563–578, Mar. 2010.
[31] W. P. Tay, J. N. Tsitsiklis, and M. Z. Win, "Bayesian detection in bounded height tree networks," *IEEE Trans. Signal Process.*, vol. 57, no. 10, pp. 4042–4051, Oct. 2009.
[32] P. Addesso, S. Marano, and V. Matta, "Estimation of target location via likelihood approximation in sensor networks," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1358–1368, Mar. 2010.
[33] T.-Y. Wang, Y. S. Han, B. Chen, and P. K. Varshney, "A combined decision fusion and channel coding scheme for distributed fault-tolerant classification in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 7, pp. 1695–1705, 2006.
[34] C. Yao, P.-N. Chen, T.-Y. Wang, Y. S. Han, and P. K. Varshney, "Performance analysis and code design for minimum Hamming distance fusion in wireless sensor networks," *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1716 –1734, May 2007.
[35] P. K. Varshney, *Distributed Detection and Data Fusion*. New York: Springer, 1997.



Chun-Yi Wei (M'08) received the B.S. and M.S. degrees in Communications Engineering from National Chiao-Tung University, Taiwan, in 2000 and 2002, respectively. In 2004, he began to pursue his Ph.D degree with the Communications Group of the School of Electronics and Computer Science, University of Southampton, UK. In 2008, he received the Ph.D. degree in Wireless Communications from University of Southampton, UK.

From 2008, he is an assistant professor in Department of Communications Engineering at National Taipei University, Taiwan. His current research interests include the wireless networks and mobile systems. Since 2012, he works closely with the industry to contribute the standards maintained by the community of the 3rd Generation Partnership Project (3GPP).

Po-Ning Chen (S'93-M'95-SM'01) was born in Taipei, R.O.C. in 1963. He received the B.S. and M.S. degrees in electrical engineering from National Tsing-Hua University, Taiwan, in 1985 and 1987, respectively, and the Ph.D. degree in electrical engineering from University of Maryland, College Park, in 1994.

From 1985 to 1987, he was with Image Processing Laboratory in National Tsing-Hua University, where he worked on the recognition of Chinese characters. During 1989, he was with Star Tech. Inc., where he focused on the development of finger-print recognition systems. After the reception of Ph.D. degree in 1994, he jointed Wan Ta Technology Inc. as a vice general manager, conducting several projects on Point-of-Sale systems. In 1995, he became a research staff in Advanced Technology Center, Computer and Communication Laboratory, Industrial Technology Research Institute in Taiwan, where he led a project on Java-based Network Managements. Since 1996, he has been an Associate Professor in Department of Communications Engineering at National Chiao-Tung University, Taiwan, and was promoted to a full professor since 2001. He was elected to be the Chair of IEEE Communications Society Taipei Chapter in 2006 and 2007, during which IEEE ComSoc Taipei Chapter won the 2007 IEEE ComSoc Chapter Achievement Awards (CAA) and 2007 IEEE ComSoc Chapter of the Year (CoY). He has served as the chairman of Department of Communications Engineering, National Chiao-Tung University, during 2007-2009. From 2012-2015, he becomes the associate chief director of Microelectronics and Information Systems Research Center, National Chiao Tung University, Taiwan, R.O.C.

Dr. Chen received the annual Research Awards from National Science Council, Taiwan, R.O.C., five years in a row since 1996. He then received the 2000 Young Scholar Paper Award from Academia Sinica, Taiwan. His Experimental Handouts for the course of Communication Networks Laboratory have been awarded as the Annual Best Teaching Materials for Communications Education by Ministry of Education, Taiwan, R.O.C., in 1998. He has been selected as the Outstanding Tutor Teacher of National Chiao-Tung University in 2002, 2013 and 2014. He was also the recipient of Distinguished Teaching Award from College of Electrical and Computer Engineering, National Chiao-Tung University, Taiwan, in 2003 and 2014. His research interests generally lie in information and coding theory, large deviation theory, distributed detection and sensor networks.

Yunghsiang S. Han (S'90-M'93-SM'08-F'11) was born in Taipei, Taiwan, 1962. He received B.Sc. and M.Sc. degrees in electrical engineering from the National Tsing Hua University, Hsinchu, Taiwan, in 1984 and 1986, respectively, and a Ph.D. degree from the School of Computer and Information Science, Syracuse University, Syracuse, NY, in 1993. He was from 1986 to 1988 a lecturer at Ming-Hsin Engineering College, Hsinchu, Taiwan. He was a teaching assistant from 1989 to 1992, and a research associate in the School of Computer and Information Science, Syracuse University from 1992 to 1993. He was, from 1993 to 1997, an Associate Professor in the Department of Electronic Engineering at Hua Fan College of Humanities and Technology, Taipei Hsien, Taiwan. He was with the Department of Computer Science and Information Engineering at National Chi Nan University, Nantou, Taiwan from 1997 to 2004. He was promoted to Professor in 1998. He was a visiting scholar in the Department of Electrical Engineering at University of Hawaii at Manoa, HI from June to October 2001, the SUPRIA visiting research scholar in the Department of Electrical Engineering and Computer Science and CASE center at Syracuse University, NY from September 2002 to January 2004 and July 2012 to June 2013, and the visiting scholar in the Department of Electrical and Computer Engineering at University of Texas at Austin, TX from August 2008 to June 2009. He was with the Graduate Institute of Communication Engineering at National Taipei University, Taipei, Taiwan from August 2004 to July 2010. From August 2010 to January 2017, he was with the Department of Electrical Engineering at National Taiwan University of Science and Technology as Chair Professor. Now he is with School of Electrical Engineering & Intelligentization at Dongguan University of Technology, China. He is also a Chair Professor at National Taipei University from February 2015. His research interests are in error-control coding, wireless networks, and security.

Dr. Han was a winner of the 1994 Syracuse University Doctoral Prize and a Fellow of IEEE. One of his papers won the prestigious 2013 ACM CCS Test-of-Time Award in cybersecurity.

Pramod K. Varshney (S'72-M'77-SM'82-F'97) was born in Allahabad, India, on July 1, 1952. He received the B.S. degree in electrical engineering and computer science (with highest hons.), and the M.S. and Ph.D. degrees in electrical engineering from the University of Illinois at Urbana-Champaign, Champaign, IL, USA, in 1972, 1974, and 1976, respectively. Since 1976, he has been with Syracuse University, Syracuse, NY, USA, where he is currently a Distinguished Professor of electrical engineering and computer science and the Director of CASE: Center for Advanced Systems and Engineering. He served as the Associate Chair of the department from 1993 to 1996. He is also an Adjunct Professor of Radiology at Upstate Medical University, Syracuse, NY. His current research interests include distributed sensor networks and data fusion, detection and estimation theory, wireless communications, image processing, radar signal processing, and remote sensing. He has published extensively. He is the author of Distributed Detection and Data Fusion (Springer-Verlag, 1997).

Dr. Varshney was a James Scholar, a Bronze Tablet Senior, and a Fellow while at the University of Illinois. He is a member of Tau Beta Pi and received the 1981 ASEE Dow Outstanding Young Faculty Award. He was elected to the grade of Fellow of the IEEE in 1997 for his contributions in the area of distributed detection and data fusion. He was the Guest Editor of the Special Issue on Data Fusion of the Proceedings of the IEEE, January 1997. In 2000, he received the Third Millennium Medal from the IEEE and the Chancellor's Citation for exceptional academic achievement at Syracuse University. He received the IEEE 2012 Judith A. Resnik Award, Doctor of Engineering Honoris causa from Drexel University in 2014, and the ECE Distinguished Alumni Award from the University of Illinois in 2015. He is on the Editorial Boards of the Journal on Advances in Information Fusion and IEEE Signal Processing Magazine. He was the President of International Society of Information Fusion during 2001.