Secure Type-Based Multiple Access

Hyoungsuk Jeon, *Member, IEEE*, Daesung Hwang, *Student Member, IEEE*, Jinho Choi, *Senior Member, IEEE*, Hyuckjae Lee, *Member, IEEE*, and Jeongseok Ha, *Member, IEEE*

***Abstract*—We consider data confidentiality in a distributed detection scenario with a type-based multiple-access (TBMA) protocol where a large set of sensors sends local measurements to an ally fusion center (FC) over an insecure wireless medium called the main channel. Then, the ally FC makes a final decision to the physical environment. Although many wireless sensor networks are mission-specific and need data confidentiality due to the broadcast nature of wireless transmission, it can be easily wiretapped by unauthorized enemy FCs through eavesdropping channels. We propose a novel TBMA protocol called secure TBMA which provides data confidentiality by taking advantage of inherent properties of wireless channels, namely randomness and independence of the main and eavesdropping channels. In particular, the secure TBMA activates sensors having strong and weak main channel gains and makes the sensors follow different reporting rules based on the magnitudes of their channel gains. The reporting rules are carefully designed to confuse the enemy FC. The proposed secure TBMA delivers unconditional/perfect secrecy and does not assume any superiority of the ally FC over the enemy FC in terms of computational capability, secret key, and so on. For Rayleigh fading channels, we analyze the performance of the secure TBMA at both enemy and ally FCs by investigating conditions for perfect secrecy and an error exponent of detection error probability, respectively. On the one hand, the analysis at the enemy FC provides a design criterion of the reporting rules to achieve perfect secrecy. On the other hand, the analysis of the error exponent carried out with a Gaussian approximation shows that perfect secrecy is achievable at a marginal cost in detection error performance. All our claims are also verified with simulation results which have good matches with the analysis.**

***Index Terms*—Distributed detection, eavesdropping, error exponents, multiuser diversity, perfect secrecy, type-based multiple access (TBMA), wireless sensor networks.**

I. Introduction

A. Motivation

DISTRIBUTED detection in wireless sensor networks (WSNs) has become increasingly popular thanks to recent advances in microelectromechanical systems that make inexpensive, low-power sensors possible [1]. In distributed detection, sensors are spread over a certain area to sense physical phenomena in a distributed fashion. Each sensor processes the collected information and transmits it over wireless channels to a fusion center (FC), which makes a global decision on the remote physical phenomena with high reliability. Since the performance of distributed detection highly depends on how the sensors and the FC collaborate with each other, a number of research studies have been focused on transmission strategies and decision-making rules.

Various efficient strategies for distributed detection have been intensively studied under the assumption of noiseless channels between sensors and the FC [2]–[5]. For noisy channels, prior works have mainly considered two channel models; parallel access channels (PACs) [6]–[9] and multiple access channels (MACs) [10]–[13]. Despite these notable contributions, a number of challenges still exist due to limited resources in sensors (e.g., power and storage capacity) and vulnerability of wireless communication links (e.g., eavesdropping and injection of fake messages).

In this paper, we are concerned with data confidentiality in a distributed detection scenario [2] with a type-based multiple-access (TBMA) protocol [11]–[13]. A large set of sensors in the network quantizes/compresses local measurements and sends them to an ally FC over an insecure wireless medium called the *main* channel. The ally FC collects the measurements and makes a final decision about the physical environment. We assume that a malicious FC, called an enemy FC, is located in the vicinity of the ally FC and tries to obtain the local measurements reported from the sensors through an *eavesdropping* channel. This threat is known as *passive eavesdropping* or *traffic analysis* and is frequently considered in both commercial applications charging service fees (e.g., customized monitoring service) and military applications handling confidential information (e.g., detecting an intruder in a battlefield). In a conventional approach for secure transmission, it is conceivable that the sensors transmit their data in the form of cyphertext to prevent eavesdropping. However, due to limited processing speed, storage capacity, and energy resources, asymmetric cryptography such as the Rivest–Shamir–Adleman algorithm or Diffie–Hellman key agreement protocol is often considered too demanding in terms of processing power [14]. Thus symmetric cryptographic solutions such as the Advanced Encryption Standard are more appropriate for WSNs, but such systems need to deal with key management and distribution issues [15], [16]. Likewise, technical difficulties may become more challenging as the size of WSNs grows.

Recently, efficient security algorithms and protocols have been proposed to accommodate sensors with constrained computational and storage resources [17]–[21]. In particular, the authors in [20], [21] introduce probabilistic enciphers to

Manuscript received September 28, 2010; revised April 15, 2011; accepted May 19, 2011. Date of publication May 31, 2011; date of current version August 17, 2011. This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0003226) and by EPSRC-DSTL under Grant EP/H011919/1. The material in this work was presented at the IEEE Information Theory Workshop (ITW), Dublin, Ireland, August 2010. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wade Trappe.

H. Jeon, D. Hwang, H. Lee, and J. Ha are with the Department of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon, 305-701, Korea (e-mail: h.jeon@kaist.ac.kr; dshwang@kaist.ac.kr; hjlee314@kaist.ac.kr; mail2jsha@kaist.ac.kr).

J. Choi is with the School of Engineering, Swansea University, Swansea, SA2 8PP, U.K. (e-mail: j.choi@swansea.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2011.2158312

prevent eavesdropping where the enciphers deliberately induce errors in the transmitted data from the sensors. It is assumed that the statistics of enciphers (i.e., the error rate that the stochastic enciphers induce) are known only to the ally FC. On the other hand, as the enemy FC is not aware of the presence of enciphers, its performance is significantly degraded at a marginal cost to the ally FC. Although these ideas provide light security measures, the statistics of enciphers can be viewed as symmetric keys shared by both the sensors and the ally FC, and thus they cannot be free from the key distribution problem.

B. Scope of Work

In this paper, we will provide a security solution that is different from the conventional approaches based on cryptographic algorithms. We address the secure distributed detection problem of binary hypothesis testing in over-deployed WSNs where there are more sensors than needed to achieve the required performance. The local measurements of the sensors are delivered to the ally FC over an MAC which is modeled as a collection of time-varying Rayleigh fading channels from the sensors to the ally FC. Time-varying channels in over-deployed WSNs provide two key features: Energy efficiency [22] and security. The latter will be explored in this paper.

The goal of our study is to design a secure transmission scheme called *secure* TBMA for distributed detection without cryptographic algorithms. The key idea behind secure TBMA is that, instead of securing the individual wireless channels based on cryptographic algorithms, the activated sensors secure their transmissions from possible eavesdropping in a cooperative manner in which the sensors follow different reporting rules depending on the magnitudes of their main channel gains.[1] We categorize sensors into three subgroups in accordance with their main channel gains: 1) Sensors with strong main channels, 2) sensors with weak main channels, and 3) the remaining sensors. The first two subgroups will be called *strong* and *weak* sets, respectively. The sensors in the strong set report their measurements as they would in conventional TBMA protocols, whereas the ones in the weak set aim to confuse the enemy FC. Although the signals from the strong set overwhelm the ones from the weak set at the ally FC, it should be noted that they all arrive at the enemy FC with statistically equal strength due to the independence between the main and eavesdropping channels. Thus, roughly to say, we design the reports from the two different sets such that they arrive at the enemy FC with equal strength and contradict each other, which causes confusion at the enemy FC. Meanwhile, in the ally FC, the reports from the strong set dominate the ones from the weak set, and thus the ally FC can correctly decide on the target status. The secure TBMA protocol exploits two key properties of wireless channels: 1) The variation of channel gains grows with the number of sensors increases, also referred to as the *multiuser diversity* [23], and 2) the main and eavesdropping channels are statistically independent when ally and enemy FCs are more than a few wavelengths apart. Multiuser diversity ensures that the gap between channel gains of the strong and weak sets can increase with a growing number of sensors at a fixed size of the strong and weak sets, which further diminishes the interference from the weak set at the ally FC.

We show that it is possible to design reporting rules for the strong and weak sets such that the enemy FC is totally ignorant of the transmitted information, i.e., *perfect secrecy* [24]. Perfect secrecy is a much stronger notion than computational security [17]–[19], mean square error [20], or detection error probability (DEP) [21]. No matter what decision rule the enemy FC adopts, the enemy FC is unable to extract any information from the received signals. We denote by T and W a random variable of target status and the sufficient statistics from the received signals at the enemy FC, respectively. The level of security can be measured by an information theoretic measure, called conditional entropy or equivocation, and for perfect secrecy, we must have

$$H(T|W) \leq H(T) \tag{1}$$

where $H(\cdot|\cdot)$ and $H(\cdot)$ are conditional entropy (or equivocation) and entropy, respectively. Perfect secrecy is achieved when the relation (1) is satisfied with equality, which implies the eavesdropper has information about the target, if it knows, only from the *a prior* probabilities of the target values not from eavesdropping. In particular, if all the target values are equally probable, $H(T)$ is also maximized and we have

$$H(T|W) = \log|\mathcal{T}|$$

where $\mathcal{T}$ is the sample space of the random variable T, and $|\mathcal{T}|$ is the cardinality of $\mathcal{T}$. We propose a design criterion of the reporting rules to achieve perfect secrecy for an asymmetric observation channel through which the sensors measure the physical phenomena. The symmetric case is also included as a special case of our work.

To evaluate the performance at the ally FC, we analyze an error exponent of the DEP with a Gaussian approximation which allows us to characterize the asymptotic behaviors of the error exponent in a closed form and thus quantify the effect of the weak set on detection performance in an analytic way. The analysis shows that perfect secrecy is achievable at a marginal cost in the DEP at the ally FC. All our claims are also verified with simulation results.

Notation

Table I introduces the notation frequently used in the paper. We use bold letters to denote vectors, and the transpose operator is denoted by the symbol $(\cdot)^T$.

C. Organization

The remaining part of this paper is organized as follows. In Section II, we introduce the system model in our work. Details of the proposed secure TBMA are also given in this section. In Section III, we design reporting rules for secure transmission, and then analyze the resulting performance at the ally and enemy FCs. We investigate the DEP and equivocation as the performance measures at the ally and enemy FCs, respectively. In Section IV, our analytic results are confirmed by Monte Carlo

[1]We will use channel gain and magnitude of channel gain interchangeably hereafter if there is no risk for confusion. We will also call *main* channels with strong and weak channel gains in magnitude as *strong* and *weak* channels.

TABLE I
GLOSSARY OF NOTATIONS

Notation	Definition
$\theta \in \{\theta_0, \theta_1\}$	Unknown target
$p(\theta_i)$	*A prior* probability of θ_i
X_ℓ	Local measurements of the ℓ-th sensor
M	Number of quantization levels
N	Number of deployed sensors
$\mathbf{p}_{\theta_i} = [p_{\theta_i}(0) \cdots p_{\theta_i}(M-1)]^T$	Conditional probability mass function of local measurements given $\theta = \theta_i$
h_l^A (h_l^E)	Channel gain from the l-th sensor to the ally (enemy) FC
τ_S (τ_W)	Threshold to determine the strong (weak) channel gain
$\bar{\mathcal{S}}_S$ ($\bar{\mathcal{S}}_W$)	Index set of the sensors with strong (weak) channel gains
$\bar{L}_S$ ($\bar{L}_W$)	Number of activated sensors in $\bar{\mathcal{S}}_S$ ($\bar{\mathcal{S}}_W$), i.e. $\bar{L}_S = \lvert\bar{\mathcal{S}}_S\rvert$ ($\bar{L}_W = \lvert\bar{\mathcal{S}}_W\rvert$)
$\mathcal{S}_S$ ($\mathcal{S}_W$)	Index sets of the activated sensors in $\bar{\mathcal{S}}_S$ ($\bar{\mathcal{S}}_W$)
L_S (L_W)	Number of activated sensors in $\mathcal{S}_S$ ($\mathcal{S}_W$) , i.e. $L_S = \lvert\mathcal{S}_S\rvert$ ($L_W = \lvert\mathcal{S}_W\rvert$)
L	Total number of activated sensors, i.e. $L = L_S + L_W$
$\{\psi_0, \ldots, \psi_{M-1}\}$	Set of predetermined orthonormal waveforms
$b(m)$	Bijective mapping function from a set of $\{0, \cdots, M-1\}$ to itself
$\mathbf{q}_S = [q_S(0) \cdots q_S(M-1)]^T$	Activation rate vector for the sensors in $\bar{\mathcal{S}}_S$
$\mathbf{q}_W = [q_W(0) \cdots q_W(M-1)]^T$	Activation rate vector for the sensors in $\bar{\mathcal{S}}_W$
$\mathbf{T}^A = [T^A(0) \cdots T^A(M-1)]^T$	Type statistics at the ally FC
$\mathbf{T}^E = [T^E(0) \cdots T^E(M-1)]^T$	Type statistics at the enemy FC
$f(\mathbf{T}^A\lvert\theta_i)$ ($f(\mathbf{T}^E\lvert\theta_i)$)	Conditional probability density function of the ally (enemy) FC given $\theta = \theta_i$
N_m^S (N_m^W)	Number of sensors transmitting ψ_m in $\mathcal{S}_S$ ($\mathcal{S}_W$)
K_m	Total number of sensors transmitting ψ_m, i.e. $K_m = N_m^S + N_m^W$
p_S (p_W)	Probability that a sensor is in $\bar{\mathcal{S}}_S$ ($\bar{\mathcal{S}}_W$)
$\tilde{p}_{S_i}$ ($\tilde{p}_{W_i}$)	Probability that a sensor is in $\mathcal{S}_S$ ($\mathcal{S}_W$) given $\theta = \theta_i$

simulations. Finally, we summarize our results and discuss future research directions in Section V.

II. SYSTEM MODEL AND TRANSMISSION STRATEGY

In this section, we present the system model for a WSN that performs distributed detection for binary hypothesis testing and propose a secure transmission strategy based on the TBMA.

Fig. 1 illustrates the system model for the WSN with secure transmission from sensors to the ally FC in the presence of the enemy FC. There are N sensors observing an unknown target $\theta \in \{\theta_0, \theta_1\}$ through statistically and temporally independent and identically distributed (i.i.d.) channels.[2] The *a prior* probabilities of θ_0 and θ_1 are denoted by $p(\theta_0)$ and $p(\theta_1)$, respectively. We denote the local measurement to the ℓth sensor ($\ell \in \{1, \ldots, N\}$) by X_ℓ which is quantized to M levels[3] with a conditional probability mass function (pmf), $\mathbf{p}_{\theta_i} = [p_{\theta_i}(0) \cdots p_{\theta_i}(M-1)]^T, i \in \{0, 1\}$ whose associated discrete memoryless channel (DMC) will be called the *observation channel*.

In Fig. 1, there are two kinds of communication channels: 1) from sensors to the ally FC; and 2) from sensors to the enemy FC, called the *main* and *eavesdropping* channels, respectively. We assume that the main and eavesdropping channel gains are i.i.d. and follow circularly symmetric complex Gaussian (CSCG) distributions

$$h_\ell^A = \alpha_\ell^A e^{j\phi_\ell^A}, h_\ell^E = \alpha_\ell^E e^{j\phi_\ell^E} \sim \mathcal{CN}\left(0, \sigma_h^2\right), \quad \forall\, \ell \qquad (2)$$

[2]Although this assumption is only valid in some limited scenarios, we mainly adopt it for analytical tractability. If this is relaxed to the non-i.i.d. case, our analysis needs to be generalized, and we leave it as our future work.

[3]Throughout this paper, we do not consider how to quantize measurements at local sensors.

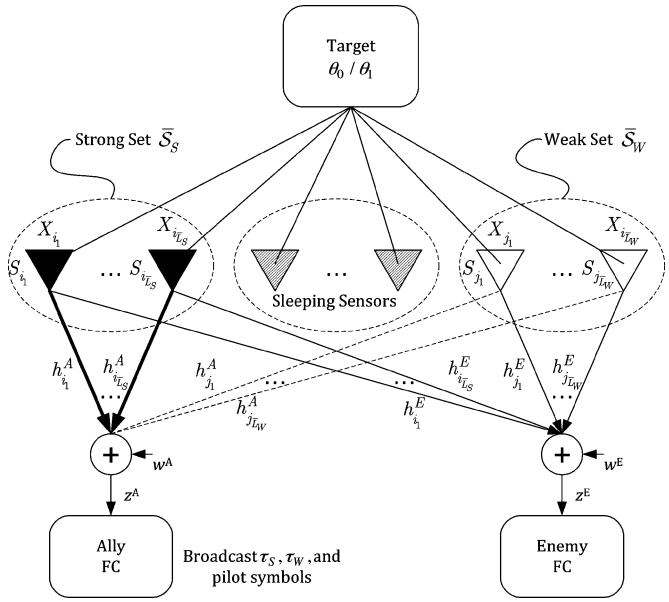

Fig. 1. WSN with ally and enemy FCs: The sensors corresponding to the indices in $\bar{\mathcal{S}}_S = \{i_1, \ldots, i_{\bar{L}_S}\}$ and $\bar{\mathcal{S}}_W = \{j_1, \ldots, j_{\bar{L}_W}\}$ have strong and weak main channel gains, respectively. The strong and weak main channels are represented as thick solid and dotted lines, respectively. The eavesdropping channels are represented as thin solid lines. The received signal z^A and z^E are corrupted by i.i.d. Gaussian noises, w^A and w^E, respectively.

where h_ℓ^A $\left(h_\ell^E\right)$ is the channel gain from the ℓth sensor node to the ally (enemy) FC, and amplitude $\alpha_\ell^A(\alpha_\ell^E)$ and phase ϕ_ℓ^A (respectively, ϕ_ℓ^E) follow the Rayleigh distribution and the uniform distribution over $[-\pi, \pi)$, respectively. Throughout the paper, we assume that the TBMA protocol is used and the enemy FC can eavesdrop signals transmitted by the sensors.

For secure TBMA, the sensors should know channel state information (CSI) of their main channels.[4] To this end, the ally FC broadcasts pilot signals and two threshold values, τ_S and τ_W, where $\tau_S > \tau_W$, and in response, the sensors transmit their measurements to the ally FC in a time-division-duplexing (TDD) manner over i.i.d. block fading channels. It is also assumed that the communication channel remains constant during a duplexing time consisting of a pilot transmission from the ally FC and transmissions from the sensors, say one block, and changes independently across blocks and sensors. Thus, the sensors can acquire CSI[5] of the main channels by taking advantage of channel reciprocity. Meanwhile, the enemy FC eavesdrops signals from the sensors through the eavesdropping channel.

As assumed in the TBMA protocol [11], the sensors simultaneously transmit their decisions to the ally FC. Due to the presence of the enemy FC in our setup shown in Fig. 1, we have to implement a certain security mechanism. To this end, we only activate some subset of sensors to transmit their local measurements by comparing their channel gains with the two threshold values, τ_S and τ_W. According to the channel condition, each sensor can decide its membership to $\bar{\mathcal{S}}_S$ or $\bar{\mathcal{S}}_W$ or no membership. $\bar{\mathcal{S}}_S$ and $\bar{\mathcal{S}}_W$ are called the strong and weak sets defined by $\bar{\mathcal{S}}_S = \{i_k | \alpha_{i_k}^A \geq \tau_S\}$ and $\bar{\mathcal{S}}_W = \{j_k | \alpha_{j_k}^A \leq \tau_W\}$, respectively. The cardinalities of $\bar{\mathcal{S}}_S$ and $\bar{\mathcal{S}}_W$ are denoted by $\bar{L}_S$ and $\bar{L}_W$, respectively. Note that the sensors in $\bar{\mathcal{S}}_S(\bar{\mathcal{S}}_W)$ have strong (respectively, weak) channel gains with respect to their main channels, not the eavesdropping channels. Thus, α_ℓ^E is not necessarily high if α_ℓ^A is high.

Among the sensors in $\bar{\mathcal{S}}_S$ and $\bar{\mathcal{S}}_W$, some sensors randomly decide to transmit their quantized measurements over the MAC by using predetermined M orthonormal waveforms denoted by $\{\psi_0, \ldots, \psi_{M-1}\}$. Each sensor in $\bar{\mathcal{S}}_S$, say sensor i, generates a uniform random variable u over $[0, 1]$ and compares it with an *activation rate* $0 \leq q_S(m) \leq 1$ when its quantized measurement is $X_i = m$. If $u < q_S(m)$, the sensor sends its measurement to the ally FC by transmitting $\sqrt{E}e^{-j\phi_i^A}\psi_m$, where the phase is compensated for coherent combining at the ally FC and E denotes the average energy consumed by each sensor node for transmission. This (random) selective transmission at the sensors plays a crucial role in providing security as will be explained later. The activation rates are designed for each level of quantization; therefore, we introduce an activation rate vector, $\mathbf{q}_S = [q_S(0)\, q_S(1) \cdots q_S(M-1)]^T$. Meanwhile, some sensors in $\bar{\mathcal{S}}_W$ are activated for transmission by comparing uniform random variables with a different activation rate vector $\mathbf{q}_W$. That is, when a sensor in $\bar{\mathcal{S}}_W$ has a measurement $b(X_i) = m$, it transmits $\sqrt{E}\psi_{b(X_i)}$ if $u < q_W(m)$ where $b(\cdot)$ is a bijective mapping from $\{0, \ldots, M-1\}$ to itself. Note that no phase compensation is made in this case. The design of activation vectors $\mathbf{q}_S$ and $\mathbf{q}_W$ and the bijective function $b(\cdot)$ will be addressed in Section III-A. We denote by $\mathcal{S}_S$ and $\mathcal{S}_W$ the sets of the activated sensors in $\bar{\mathcal{S}}_S$ and $\bar{\mathcal{S}}_W$, respectively. Thus, $\mathcal{S}_S \subseteq \bar{\mathcal{S}}_S$ and $\mathcal{S}_W \subseteq \bar{\mathcal{S}}_W$. In the end, we have $L = L_S + L_W$ activated sensors, where $L_S = |\mathcal{S}_S| \leq \bar{L}_S$ and $L_W = |\mathcal{S}_W| \leq \bar{L}_W$. The sensors neither in $\mathcal{S}_S$ nor $\mathcal{S}_W$ are dormant.

Note that the transmission from the sensors in $\mathcal{S}_W$, which is crucial for security, causes interference at the ally FC. However, the performance degradation resulting from this induced interference is negligible due to the weak channel gains as will be shown later. Our objective is to find combinations of design parameters τ_S, τ_W, $\mathbf{q}_S$, $\mathbf{q}_W$, and $b(\cdot)$ to achieve perfect secrecy against eavesdropping by the enemy FC, which will be addressed in Section III.

III. Analysis

In this section, the secure TBMA protocol is analyzed by investigating conditions for maximizing the equivocation at the enemy FC and error exponent at the ally FC. In particular, the analysis of the type statistics at the enemy FC provides a design criterion for perfect secrecy for a given observation channel. The design criterion is also derived for energy efficiency and a better detection performance at the ally FC. In the second part of this section, we quantify the performance degradation due to transmitting sensors in $\mathcal{S}_W$ through the error exponent of the DEP at the ally FC.

[4]We assume that sensors do not know the eavesdropping channel gains, since the enemy FC does not transmit any signal to the sensors to hide its presence.

[5]Thus, we consider coherent communications in this paper. Note that since the bandwidth of wireless channels in the TBMA between the sensors and FC is usually assumed to be narrow, the circuit for channel estimation and coherent communications may not be complicated and could be implemented in a compact size.

A. Enemy Fusion Center

To achieve the maximum equivocation, i.e., $H(T|W) = H(T)$, T must be statistically independent of W. In our problem setup, the type statistics $\mathbf{T}^E$ at the enemy FC is the sufficient statistics, and a binary target random variable $\theta \in \{\theta_0, \theta_1\}$ is information to be secured from eavesdropping. Thus, the necessary and sufficient condition for perfect secrecy at the enemy FC is that the conditional pdf of the type statistics under hypothesis θ_i, denoted by $f\left(\mathbf{T}^E|\theta_i\right)$, should be independent of θ_i for $i \in \{0,1\}$ [24]. In summary, what we have to do in this section is to find a combination of $\tau_S, \tau_W, \mathbf{q}_S, \mathbf{q}_W$, and $b(\cdot)$ for $f(\mathbf{T}^E|\theta_0) = f(\mathbf{T}^E|\theta_1)$. We first characterize the conditional pdf of the type statistics in terms of $\tau_S, \tau_W, \mathbf{q}_S, \mathbf{q}_W$, and $b(\cdot)$, and then establish design rules of them for perfect secrecy.

According to the transmission strategy discussed in Section II, the received signal at the enemy FC, denoted by z^E, can be expressed in terms of a weighted sum of the transmitted signals as follows:

$$\begin{aligned} z^E &= \sqrt{E}\sum_{i\in\mathcal{S}_S} h_i^E e^{-j\phi_i^A}\psi_{X_i} \\ &\quad + \sqrt{E}\sum_{j\in\mathcal{S}_W} h_j^E \psi_{b(X_j)} + w^E \\ &\overset{\text{(a)}}{=} \sqrt{E}\sum_{i\in\mathcal{S}_S} h_i^E \psi_{X_i} + \sqrt{E}\sum_{j\in\mathcal{S}_W} h_j^E \psi_{b(X_j)} + w^E \end{aligned} \quad (3)$$

where w^E is a zero-mean CSCG random variable with variance σ^2, and the equality (a) results from the fact that $h_i^E e^{-j\phi_i^A}$ and h_i^E have the same distribution. The enemy FC obtains the type statistics $\mathbf{T}^E = \left[T_0^E, \ldots, T_{M-1}^E\right]^T$ from the output of a bank of matched filters with the impulse responses $\psi_m/\sqrt{E}$, $m = 0, \ldots, M-1$, where

$$T_m^E = \sum_{i\in\mathcal{S}_S} h_i^E 1_{(X_i=m)} + \sum_{j\in\mathcal{S}_W} h_j^E 1_{(b(X_j)=m)} + w_m^E. \quad (4)$$

Here, $1_{(x=m)}$ is the indicator function which is 1 if $x = m$ and 0 otherwise, and w_m^E is a zero-mean CSCG random variable with variance σ^2/E.

To characterize $f(\mathbf{T}^E|\theta_i)$ from (4), we introduce two random vectors: $\mathbf{N}^S = \left[N_0^S, \ldots, N_{M-1}^S\right]^T$ and $\mathbf{N}^W = \left[N_0^W, \ldots, N_{M-1}^W\right]^T$, where $N_m^S = \sum_{i\in\mathcal{S}_S} 1_{(X_i=m)}$ and $N_m^W = \sum_{j\in\mathcal{S}_W} 1_{(b(X_j)=m)}$ are the numbers of sensors transmitting the mth waveform ψ_m in $\mathcal{S}_S$ and $\mathcal{S}_W$, respectively. Then, $f(\mathbf{T}^E|\theta_i)$ is rewritten as

$$\begin{aligned} f(\mathbf{T}^E|\theta_i) &= \sum_{K_0=0}^{N}\sum_{K_1=0}^{N_1}\cdots\sum_{K_{M-1}=0}^{N_{M-1}}\sum_{N_0^W=0}^{K_0}\cdots\sum_{N_{M-1}^W=0}^{K_{M-1}} f \\ &\quad \times \left(\mathbf{T}^E|\mathbf{K},\mathbf{N}^W,\theta_i\right) p\left(\mathbf{K},\mathbf{N}^W|\theta_i\right) \end{aligned} \quad (5)$$

where $\mathbf{K} = [K_0, \ldots, K_{M-1}]^T$, $K_m = N_m^S + N_m^W$, and $N_i = N - \left(\sum_{m=0}^{i-1} K_m\right)$. Since K_m counts the number of activated sensors transmitting the mth waveform both in $\mathcal{S}_S$ and $\mathcal{S}_W$, it is the type statistics across the activated sensors. The Markov chain $\theta_i \to [X_1, \ldots, X_L] \to \left\{\mathbf{K} = \mathbf{N}^S + \mathbf{N}^W\right\} \to \{\mathbf{T}^E\}$ simplifies (5) to

$$\begin{aligned} f(\mathbf{T}^E|\theta_i) &= \sum_{K_0=0}^{N}\sum_{K_1=0}^{N_1}\cdots\sum_{K_{M-1}=0}^{N_{M-1}}\sum_{N_0^W=0}^{K_0}\cdots\sum_{N_{M-1}^W=0}^{K_{M-1}} f \\ &\quad \times \left(\mathbf{T}^E|\mathbf{K}\right) p\left(\mathbf{K},\mathbf{N}^W|\theta_i\right) \end{aligned} \quad (6)$$

where $f\left(\mathbf{T}^E|\mathbf{K},\mathbf{N}^W,\theta_i\right)$ in (5) becomes $f(\mathbf{T}^E|\mathbf{K})$. The pmf $p(\mathbf{K},\mathbf{N}^W|\theta_i)$ in (6) can be factorized as follows:

$$\begin{aligned} p\left(\mathbf{K},\mathbf{N}^W|\theta_i\right) &\overset{\text{(a)}}{=} p\left(\mathbf{N}^S,\mathbf{N}^W,L_S,L_W|\theta_i\right) \\ &= p\left(\mathbf{N}^S|\mathbf{N}^W,L_S,L_W,\theta_i\right) \\ &\quad \times p\left(\mathbf{N}^W|L_S,L_W,\theta_i\right) p\left(L_S,L_W|\theta_i\right) \\ &\overset{\text{(b)}}{=} p\left(\mathbf{N}^S|L_S,\theta_i\right) p\left(\mathbf{N}^W|L_W,\theta_i\right) \\ &\quad \times p(L_S,L_W|\theta_i) \end{aligned} \quad (7)$$

where the equality (a) is due to $L_S = \sum_m K_m - N_m^W$ and $L_W = \sum_m N_i^W$, and (b) follows from the fact that the selections of the activated sensors in $\bar{\mathcal{S}}_S$ and $\bar{\mathcal{S}}_W$ are statistically independent. The first two terms in (7) represent the probabilities of types $\mathbf{N}^S$ and $\mathbf{N}^W$ for a target value θ_i when L_S and L_W sensors are activated in $\mathcal{S}_S$ and $\mathcal{S}_W$, respectively, and the last term is the probability that the numbers of activated sensors in $\mathcal{S}_S$ and $\mathcal{S}_W$ are equal to L_S and L_W, respectively.

Now, we express the three probabilities in (7) in terms of $\mathbf{p}_{\theta_i}$, $\mathbf{q}_S$ and $\mathbf{q}_W$. For simplicity, let $\tilde{q}_{S_i}(m) = q_S(m)p_{\theta_i}(m)$ ($\tilde{q}_{W_i}(m) = q_W(m)p_{\theta_i}(m)$) which represents the probability that a sensor in $\mathcal{S}_S$ (respectively, $\mathcal{S}_W$) transmits the mth waveform under hypothesis θ_i. Thus, the sensors in $\mathcal{S}_W$ and $\mathcal{S}_S$ are activated under θ_i with the probabilities

$$\tilde{p}_{S_i} = p_S \sum_{m=0}^{M-1} \tilde{q}_{S_i}(m) = \mathbf{q}_S^T \mathbf{p}_{\theta_i} p_S$$

and

$$\tilde{p}_{W_i} = p_W \sum_{m=0}^{M-1} \tilde{q}_{W_i}(m) = \mathbf{q}_W^T \mathbf{p}_{\theta_i} p_W$$

respectively, where $p_S = \Pr\{\alpha^A > \tau_S\}$ and $p_W = \Pr\{\alpha^A < \tau_W\}$. Using the multinomial distribution, we then obtain the following relations:

$$\begin{aligned} &p\left(\mathbf{N}^S|L_S,\theta_i\right) \\ &\quad = \binom{L_S}{N_0^S,\ldots,N_{M-1}^S} \prod_{m=0}^{M-1} \left[\tilde{q}_{S_i}(m)\right]^{N_m^S} \end{aligned} \quad (8)$$

$$\begin{aligned} &p\left(\mathbf{N}^W|L_W,\theta_i\right) \\ &\quad = \binom{L_W}{N_0^W,\ldots,N_{M-1}^W} \prod_{m=0}^{M-1} \left[\tilde{q}_{W_i}\left(M-m-1\right)\right]^{N_m^W} \end{aligned} \quad (9)$$

$$\begin{aligned} &p\left(L_S,L_W|\,\theta_i\right) \\ &\quad = \binom{N}{L_S,L_W,N-L} \left(\tilde{p}_{S_i}\right)^{L_S} \left(\tilde{p}_{W_i}\right)^{L_W} \\ &\qquad \times \left(1-\tilde{p}_{S_i}-\tilde{p}_{W_i}\right)^{N-L}. \end{aligned} \quad (10)$$

Substituting (7) with the product of (8)–(10), we finally get

$$\begin{aligned} f(\mathbf{T}^E|\theta_i) &= \sum_{K_0=0}^{N}\sum_{K_1=0}^{N_1}\cdots\sum_{K_{M-1}=0}^{N_{M-1}} \frac{N!}{(N-L)!} f\left(\mathbf{T}^E|\mathbf{K}\right) \\ &\quad\times \sum_{N_0^W=0}^{K_0}\cdots\sum_{N_{M-1}^W=0}^{K_{M-1}} \frac{(1-\tilde{p}_{S_i}-\tilde{p}_{W_i})^{N-L}}{\prod_{m=0}^{M-1}K_m!} \\ &\quad\times \prod_{m=0}^{M-1}\binom{K_m}{N_m^S}\left[\tilde{p}_{S_i}\tilde{q}_{S_i}(m)\right]^{N_m^S} \\ &\quad\times \left[\tilde{p}_{W_i}\tilde{q}_{W_i}(b(m))\right]^{N_m^W} \\ &\overset{(a)}{=} \sum_{K_0=0}^{N}\sum_{K_1=0}^{N_1}\cdots\sum_{K_{M-1}=0}^{N_{M-1}} f\left(\mathbf{T}^E|\mathbf{K}\right) \\ &\quad\times \frac{N!\,(1-\tilde{p}_{S_i}-\tilde{p}_{W_i})^{N-L}}{(N-L)\prod_{m=0}^{M-1}K_m!} \\ &\quad\times \prod_{m=0}^{M-1}\left[\tilde{p}_{S_i}\tilde{q}_{S_i}(m)+\tilde{p}_{W_i}\tilde{q}_{W_i}(b(m))\right]^{K_m} \end{aligned} \tag{11}$$

where (a) follows from the fact in Appendix A. Note that we should make (11) independent of the hypothesis θ_i to achieve perfect secrecy, i.e., $f(\mathbf{T}^E|\theta_0)=f(\mathbf{T}^E|\theta_1)$. We will show that there are combinations of design parameters τ_S, τ_W, $\mathbf{q}_S$, $\mathbf{q}_W$, and $b(\cdot)$ with which perfect secrecy is accomplished.

1) Design Parameters for Perfect Secrecy: In the derivation of design rules for perfect secrecy, we also consider possible attacks based on side information. We assume that the enemy FC can estimate not only the type statistics of received signals but also side information of the secure TBMA such as L_S, L_W, and $K_0,\ldots,K_{M-1}$, which contain information about the target status. In that case, the enemy FC can gain information about θ_i by analyzing the side information. Thus, we employ the following conditions to prevent such information leakage while guaranteeing perfect secrecy against eavesdropping, $f(\mathbf{T}^E|\theta_0)=f(\mathbf{T}^E|\theta_1)$:

$$\tilde{p}_{S_0}=\tilde{p}_{S_1}\text{ and }\tilde{p}_{W_0}=\tilde{p}_{W_1} \tag{12}$$

$$\begin{aligned}&\tilde{p}_{S_0}\tilde{q}_{S_0}(m)+\tilde{p}_{W_0}\tilde{q}_{W_0}(b(m)) \\ &\quad=\tilde{p}_{S_1}\tilde{q}_{S_1}(m)+\tilde{p}_{W_1}\tilde{q}_{W_1}(b(m))\end{aligned} \tag{13}$$

for $m=0,\ldots,M-1$. The conditions in (12) are to make the activation probability of sensors in $\mathcal{S}_S(\mathcal{S}_W)$ independent of θ_i, while that in (13) ensures that the probability of activated sensors transmitting the mth waveform is independent of θ_i. Thus, if (12) and (13) are satisfied, the size of $\mathcal{S}_S(\mathcal{S}_W)$ and the number of sensors transmitting the mth waveform are not changed with respect to the target status θ_i, and the enemy FC cannot take advantage of estimating the side information of the secure TBMA. The condition in (13) imposes the following relation between $q_S(m)$ and $q_W(m)$:

$$q_W(b(m))=-\rho\frac{\mathbf{q}_S^T\mathbf{p}_{\theta_0}}{\mathbf{q}_W^T\mathbf{p}_{\theta_0}}\frac{\gamma(m)}{\gamma(b(m))}q_S(m) \tag{14}$$

where $\rho=p_S/p_W$, and $\gamma(m)=p_{\theta_0}(m)-p_{\theta_1}(m)$. As a vector form, (12) and (14) can be rewritten as

$$\mathbf{q}_S^T\mathbf{p}_{\theta_0}=\mathbf{q}_S^T\mathbf{p}_{\theta_1}\text{ and }\mathbf{q}_W^T\mathbf{p}_{\theta_0}=\mathbf{q}_W^T\mathbf{p}_{\theta_1} \tag{15}$$

$$\mathbf{q}_W=\sqrt{\rho\frac{\mathbf{q}_S^T\mathbf{p}_{\theta_0}}{\mathbf{v}^T\mathbf{p}_{\theta_0}}}\mathbf{v} \tag{16}$$

where $\mathbf{v}=[v(0)\cdots v(M-1)]^T$ and $v(b(m))=-(\gamma(m)/\gamma(b(m)))q_S(m)$. Note that since $0\le q_W(m)\le 1$ for all m, we can design $q_W(m)$ only if

$$\gamma(b(m))\gamma(m)\le 0\text{ for all }m. \tag{17}$$

This condition may be achieved by designing the bijective mapping $b(\cdot)$ and/or quantization of the local measurements which determines the pmfs $\mathbf{p}_{\theta_0}$ and $\mathbf{p}_{\theta_1}$. However, in this paper, we do not consider the local quantization and only focus on the design of $b(\cdot)$ for given $\mathbf{p}_{\theta_0}$ and $\mathbf{p}_{\theta_1}$.

While for given $\mathbf{p}_{\theta_0}$ and $\mathbf{p}_{\theta_1}$, we found the requirements for $\mathbf{q}_S$ and $\mathbf{q}_W$ in (15) and (16) and those for the bijective mapping $b(\cdot)$ in (17), the existence of such parameters is shown in Theorem 1.

Theorem 1: If $\gamma(b(m))\gamma(m)<0$ holds for all m with a bijective mapping $b(m)$, there always exist vectors $\mathbf{q}_S$ and $\mathbf{q}_W$ that guarantee perfect secrecy at the enemy FC.

Proof: If $\gamma(b(m))\gamma(m)<0$ holds for all m, we can always find $\mathbf{q}_S$ to satisfy $\mathbf{q}_S^T(\mathbf{p}_{\theta_0}-\mathbf{p}_{\theta_1})=0$. Then, for a given $\mathbf{q}_S^T\mathbf{p}_{\theta_0}=c\,(\text{constant})$, we have

$$\begin{aligned}\mathbf{q}_W^T(\mathbf{p}_{\theta_0}-\mathbf{p}_{\theta_1}) &= \sqrt{\frac{\rho c}{\mathbf{v}^T\mathbf{p}_{\theta_0}}}\mathbf{v}^T(\mathbf{p}_{\theta_0}-\mathbf{p}_{\theta_1}) \\ &= -\sqrt{\frac{\rho c}{\mathbf{v}^T\mathbf{p}_{\theta_0}}}\sum_{m=0}^{M-1}\gamma(m)q_S(m) \\ &=0\end{aligned} \tag{18}$$

which satisfies (15) and completes this proof. □

Now, we will find the requirements for τ_S and τ_W to achieve perfect secrecy. Since $q_W(m)\in[0,1]$, the equation in (16) tells that ρ is upper-bounded by

$$\rho\le\frac{\mathbf{v}^T\mathbf{p}_{\theta_0}}{\mathbf{q}_S^T\mathbf{p}_{\theta_0}(\max_m\{v(m)\})^2} \tag{19}$$

which also implies a relation between τ_S and τ_W through the definition $\rho=\Pr(\alpha^A>\tau_S)/\Pr(\alpha^A<\tau_W)$.

In summary, the conditions to achieve perfect secrecy can be found in (15) for $\mathbf{q}_S$ and $\mathbf{q}_W$ and in (17) for $b(\cdot)$. The relation between $\mathbf{q}_S$ and $\mathbf{q}_W$ is given by (16) and the upper bound on ρ by (19). Next, we can further optimize the design parameters for energy efficient in Section III-B.

2) Energy-Efficient Design: For energy efficiency, the number of activated sensors must be minimized as long as the target DEP at the ally FC is met. We address this problem by maximizing the activation probability ratio, $\max\tilde{p}_{S_i}/\tilde{p}_{W_i}=\max\rho\mathbf{q}_S^T\mathbf{p}_{\theta_0}/\mathbf{q}_W^T\mathbf{p}_{\theta_0}$. Although, by adjusting thresholds τ_S and τ_W, there are various combinations of design parameters to satisfy the target DEP in the secure TBMA, minimizing the interference induced by $\mathcal{S}_W$ is the approach to

meet the target DEP with the minimum number of activated sensors. Thus, considering the design rules for perfect secrecy, we formulate the following optimization problem:

$$\max_{\mathbf{q}_S, b\in\mathcal{B}, \tau_S, \tau_W} \rho \frac{\mathbf{q}_S^T \mathbf{p}_{\theta_0}}{\mathbf{q}_W^T \mathbf{p}_{\theta_0}} \tag{20}$$

subject to

$$\begin{aligned} \mathbf{q}_S^T \mathbf{p}_{\theta_0} &= \mathbf{q}_S^T \mathbf{p}_{\theta_1} \\ \gamma(b(m))\gamma(m) &\le 0 \text{ for all } m \\ \rho &\le \frac{\mathbf{v}^T \mathbf{p}_{\theta_0}}{\mathbf{q}_S^T \mathbf{p}_{\theta_0} (\max_m \{v(m)\})^2} \\ \mathbf{q}_W &= \sqrt{\rho \frac{\mathbf{q}_S^T \mathbf{p}_{\theta_0}}{\mathbf{v}^T \mathbf{p}_{\theta_0}}} \mathbf{v} \end{aligned}$$

where $\mathcal{B}$ is the set of all bijective mappings from $\{0, \ldots, M-1\}$ to itself.

For the selection of τ_S and τ_W, achieving the bound of ρ is the best way to maximize (20) for any given $\mathbf{q}_S$ and $b(\cdot)$ since the changes of two thresholds only affect ρ in (20). In particular, since the sensors in $\mathcal{S}_W$ consume energy only for the security purpose, it is desirable to maximize (20) in a way that we minimize the size of $\mathcal{S}_W$ by decreasing τ_W until the requirements for perfect secrecy are met. This choice also selects the sensors in $\mathcal{S}_W$ to have smaller main channel gains and thus makes the level of interference at the ally FC further reduced.

However, note that it is not easy to jointly optimize (20) since $\mathbf{q}_S$ and $b(\cdot)$ are heavily intertwined in the objective function. Thus, as a suboptimal way, we let $\mathbf{q}_S = \mathbf{1}$ to make $\bar{\mathcal{S}}_S = \mathcal{S}_S$ where $\mathbf{1}$ is the all-one vector of length m. The requirement in (15) is then valid as

$$\mathbf{1}^T \cdot (\mathbf{p}_{\theta_0} - \mathbf{p}_{\theta_1}) = \sum_m p_{\theta_0}(m) - \sum_m p_{\theta_1}(m) = 0.$$

This is a reasonable choice since our purpose is to minimize the number of activated sensors in the secure TBMA. Suppose that $q_S(m) < 1$ for some m. Then, some of sensors in $\bar{\mathcal{S}}_S$ are not activated, and to achieve the target DEP, $\bar{\mathcal{S}}_S$ should have more sensors by decreasing the threshold τ_S than the case with $\mathbf{q}_S = \mathbf{1}$. Since the smaller threshold includes the sensors in $\bar{\mathcal{S}}_S$ with weaker channel gains, more sensors must be activated to achieve the same DEP. For $\mathbf{q}_S = \mathbf{1}$, the design of $b(\cdot)$ is then tuned to maximize the ratio $\tilde{p}_{S_i}/\tilde{p}_{W_i}$.

3) Example 1 (Design of $b(\cdot)$): Consider an observation channel, $\mathbf{p}_{\theta_0} = [0.4\, 0.3\, 0.2\, 0.1]^T$ and $\mathbf{p}_{\theta_1} = [0.1\, 0.2\, 0.5\, 0.2]^T$. The bijective mapping $b(\cdot)$ can be designed through an exhaustive search. Since the number of quantization levels M is 4, there are $4! = 24$ mappings among which the mappings listed in Table II satisfy the condition in (17). The parameters ρ and $\tilde{p}_{S_i}/\tilde{p}_{W_i}$ are listed in the last two columns of Table II for each mapping, and the one in the third row is shown to be the best choice.[6]

We now consider a special case where the observation channel is symmetric, $p_{\theta_0}(m) = p_{\theta_1}(M-m-1), \forall\, m$.

[6]In some cases, multiple choices of $b(\cdot)$ can be obtained. For example, if $\mathbf{p}_{\theta_0} = [0.4\ 0.3\ 0.2\ 0.1]^T$ and $\mathbf{p}_{\theta_1} = [0.1\ 0.2\ 0.4\ 0.3]^T$, then all possible mappings have the same values of $\tilde{p}_{S_i}/\tilde{p}_{W_i}$

TABLE II
BIJECTIVE MAPPINGS FOR $\mathbf{p}_{\theta_0} = [0.4\ 0.3\ 0.2\ 0.1]^T$, $\mathbf{p}_{\theta_1} = [0.1\ 0.2\ 0.5\ 0.2]^T$ AND $\mathbf{q}_S = \mathbf{1}$

$b(0)$	$b(1)$	$b(2)$	$b(3)$	ρ	$\tilde{p}_{S_i}/\tilde{p}_{W_i}$
2	3	1	0	0.1481	0.3333
3	2	1	0	0.1556	0.3333
2	3	0	1	1.0000	1.0000
3	2	0	1	0.1185	0.3333

Proposition 1: For $\mathbf{q}_S = \mathbf{1}$, $\tilde{p}_{S_i}/\tilde{p}_{W_i}$ is upper bounded by 1. If the observation channel is symmetric, then the mapping $b(m) = M - m - 1$ achieves the equality, $\tilde{p}_{S_i}/\tilde{p}_{W_i} = 1$.

Proof: For given $\mathbf{q}_S = \mathbf{1}$, we first find an upper bound on ρ. Denote by $b^*(\cdot)$ a bijective mapping that maximizes (20) and satisfies (17). Then, we have the following inequality:

$$\begin{aligned} \rho &\le \max_{b\in\mathcal{B}} \frac{\mathbf{v}^T \mathbf{p}_{\theta_0}}{(\max_m \{v(m)\})^2} \\ &= \frac{1}{(v_{\max})^2} \sum_{m=0}^{M-1} v(b^*(m)) p_{\theta_0}(b^*(m)) \\ &\le \frac{1}{(v_{\max})^2} \sum_{m=0}^{M-1} v_{\max} p_{\theta_0}(m) = \frac{1}{v_{\max}} \end{aligned} \tag{21}$$

where $v_{\max} = \max_m \{v(m)\}$. If we let $\mathcal{M} = \{m : |\gamma(m)| \ge |\gamma(n)|, \forall\, n \ne m\}$, then

$$v_{\max} \ge \max_{m\in\mathcal{M}} v(b^*(m)) = \max_{m\in\mathcal{M}} -\frac{\gamma(m)}{\gamma(b^*(m))} \ge 1.$$

Thus, $\rho \le (1/v_{\max}) \le 1$, where the equality holds when $\gamma(m) = -\gamma(b^*(m))$ (i.e., $\mathbf{v} = \mathbf{1}$), which is possible with $b^*(m) = M - m - 1$. Thus, we can achieve $\rho = 1$. Then, $\mathbf{q}_W = \sqrt{\rho(\mathbf{q}_S^T \mathbf{p}_{\theta_0}/\mathbf{v}^T \mathbf{p}_{\theta_0})}\mathbf{v} = \mathbf{1}$, and we have $\tilde{p}_{S_i}/\tilde{p}_{W_i} = 1$. □

Remark 1: Proposition 1 shows that for a symmetric observation channel, all sensors in $\bar{\mathcal{S}}_S$ and $\bar{\mathcal{S}}_W$ are activated, and the reports from the two sets are exactly the opposite of each other.

The energy efficiency can be further studied by investigating power control strategies although they are not addressed in this paper. Finally, to better understand our design rules, we provide a couple of examples for asymmetric and symmetric observation channels.

4) Example 2 (Asymmetric Observation Channel): Consider the observation channel in Example 1. As we noted, maximizing ρ with $\mathbf{q}_S = \mathbf{1}$ is an energy efficient design that achieves perfect secrecy. If we select the third row in Table II as the mapping $b(\cdot)$, then we have $\mathbf{q}_W = \mathbf{1}$. For the selection of τ_S and τ_W, we need the target DEP and performance evaluations at the ally FC which will be done in Section IV. In Fig. 5, to achieve a target DEP of 10^{-3}, we need $p_S = \Pr(\alpha^A > \tau_S)$ of 0.17 and easily have $\tau_S = 1.3311$ from the cumulative distribution function for the Rayleigh distribution with mean $\sqrt{\pi}/2$. Since $\rho = p_S/p_W = 1$, we have $p_W = 0.17$ and $\tau_W = 0.4317$.

5) Example 3 (Symmetric Observation Channel): Suppose that a symmetric channel is given by $\mathbf{p}_{\theta_0} = [0.4\ 0.3\ 0.2\ 0.1]^T$ and $\mathbf{p}_{\theta_1} = [0.1\ 0.2\ 0.3\ 0.4]^T$. For $\mathbf{q}_S = \mathbf{1}$, the best mapping is $b(m) = M - m - 1$ and $\mathbf{q}_W = \mathbf{1}$ with $\rho = \rho_{\max} = 1$. The parameters τ_S and τ_W may be selected by evaluations of the DEP at the ally FC as in Example 2.

B. Ally Fusion Center

We derive the error exponent of the DEP in order to evaluate the detection performance at the ally FC. Although large deviation (LD) theory [25] is the conventional approach to calculate the error exponent, it is not mathematically tractable to analyze the performance of secure TBMA. Thus, a different approach is employed in this paper. We first approximate the type statistics as a Gaussian distribution applying the central limit theorem (CLT) and then adopt the Chernoff bound to analyze the error exponent of the DEP which allows us to understand the asymptotic behavior of the type statistics as N grows. In particular, we will design a detection rule and analyze the asymptotic behavior of the DEP defined as $P_e = p(\hat{\theta}_1|\theta_0)p(\theta_0) + p(\hat{\theta}_0|\theta_1)p(\theta_1)$. We begin with the received signal at the ally FC over the MAC which is modeled as the superposition of the transmitted signals as follows:

$$z^A = \sqrt{E}\sum_{i\in\mathcal{S}_S}\alpha_i^A\psi_{X_i} + \sqrt{E}\sum_{j\in\mathcal{S}_W}h_j^A\psi_{b(X_j)} + w^A \quad (22)$$

where w^A is a zero-mean CSCG random variable with variance σ^2. The real part of the matched filter output at the ally FC is given by

$$\begin{aligned}\mathbf{T}^A &= \frac{1}{\sqrt{E}}\left[\langle z^A,\psi_0\rangle,\ldots,\langle z^A,\psi_{M-1}\rangle\right]^T \\ &= \sum_{i\in\mathcal{S}_S}\tilde{\alpha}_i^A\mathbf{e}_{X_i} + \sum_{j\in\mathcal{S}_W}\tilde{h}_j^A\mathbf{e}_{b(X_j)} + \mathbf{w}^A \end{aligned} \quad (23)$$

where $\langle z^A,\psi_m\rangle$ is the real part of the matched filter output with ψ_m, $\tilde{\alpha}_i^A$ and $\tilde{h}_j^A$ are the real parts of the channel gains for $i \in \mathcal{S}_S$ and $j \in \mathcal{S}_W$, respectively, $\mathbf{e}_X$ is a standard basis whose value is 1 at $X \in \{0,\ldots,M-1\}$ and 0 otherwise, and $\mathbf{w}^A \sim \mathcal{N}\left(0,\sigma^2/(2E)\,\mathbf{I}\right)$.

For the Bayesian setup, the optimal decision rule is based on the maximum likelihood test with the decision regions as follows:

$$\begin{aligned}\Gamma_0 &= \left\{\mathbf{T}^A\in\mathbb{R}^M\left|\frac{f\left(\mathbf{T}^A|\theta_1\right)}{f\left(\mathbf{T}^A|\theta_0\right)} < \frac{p(\theta_0)}{p(\theta_1)}\right.\right\} \\ \Gamma_1 &= \mathbb{R}^M\setminus\Gamma_0 \end{aligned} \quad (24)$$

where $f\left(\mathbf{T}^A|\theta_i\right)$ is the conditional pdf of $\mathbf{T}^A$ under hypothesis θ_i. The ally FC accepts θ_i when the matched filter output $\mathbf{T}^A$ is in Γ_i. The Gaussian approximation can be used to characterize these decision regions in an analytic way, and thereby we can evaluate the error exponent of the DEP at the ally FC.

Since the numbers of activated sensors in $\mathcal{S}_S$ and $\mathcal{S}_W$ are random variables, the standard multivariate CLT cannot be directly applied to our model. In [13], this problem is solved by using the CLT with random number summands in [26]. We use a different approach by introducing an auxiliary random vector $\mathbf{y}_\ell$ that represents the ℓth sensor's transmitted signal which is one of the following three different types according to its involved set:

$$\mathbf{y}_\ell = \begin{cases}\tilde{\alpha}_\ell^A\mathbf{e}_{X_\ell} & \text{with prob. } \tilde{p}_{S_i} \\ \tilde{h}_\ell^A\mathbf{e}_{b(X_\ell)} & \text{with prob. } \tilde{p}_{W_i} \quad \text{for } i=0,1 \\ 0 & \text{with prob. } 1-\tilde{p}_{S_i}-\tilde{p}_{W_i}.\end{cases} \quad (25)$$

The mean vector and covariance matrix, denoted by $\mathbb{E}\{\mathbf{y}_\ell\}$ and $\mathrm{Cov}(\mathbf{y}_\ell)$, are, respectively, given by

$$\begin{aligned}&\mathbb{E}\{\mathbf{y}_\ell\} \\ &\quad = \tilde{p}_{S_i}\mu_S\tilde{\mathbf{q}}_{S_i} \end{aligned} \quad (26)$$

$$\begin{aligned}&\mathrm{Cov}(\mathbf{y}_\ell) \\ &\quad = \mathbb{E}\left\{\left(\mathbf{y}_\ell - \tilde{p}_{S_i}\mu_S\tilde{\mathbf{q}}_{S_i}\right)\left(\mathbf{y}_\ell - \tilde{p}_{S_i}\mu_S\tilde{\mathbf{q}}_{S_i}\right)^T\right\} \\ &\quad = \tilde{p}_{S_i}\left(\mu_S^2+\sigma_S^2\right)\mathrm{Diag}\left(\tilde{\mathbf{q}}_{S_i}\right) - \tilde{p}_{S_i}^2\mu_S^2\tilde{\mathbf{q}}_{S_i}\tilde{\mathbf{q}}_{S_i}^T \\ &\qquad + \tilde{p}_{W_i}\sigma_W^2\mathrm{Diag}\left(\left[\tilde{q}_{W_i}(b(0))\ \cdots\ \tilde{q}_{W_i}(b(M-1))\right]\right) \end{aligned} \quad (27)$$

where $\tilde{\mathbf{q}}_{S_i} = [\tilde{q}_{S_i}(0)\ \cdots\ \tilde{q}_{S_i}(M-1)]^T$, μ_S is the mean of $\tilde{\alpha}_\ell^A$, and σ_S^2 and σ_W^2 are the variances of $\tilde{\alpha}_\ell^A$ and $\tilde{h}_\ell^A$, respectively. They can be derived from the pdfs of $\tilde{\alpha}_\ell^A$ and $\tilde{h}_\ell^A$ presented in Appendix B.

We model the matched filter output as the sum of i.i.d. random vectors, $\mathbf{y}_\ell$ for $\ell = 0,1,\ldots,N$, which allows us to use the standard multivariate CLT in our approximation. The vector of the type statistics in (23) is rewritten in terms of $\mathbf{y}_\ell$ as follows:

$$\mathbf{T}^A = \sum_{\ell=1}^N\mathbf{y}_\ell + \mathbf{w}^A. \quad (28)$$

Using the multivariate CLT [26], the statistics of $\sum_{\ell=1}^N\mathbf{y}_\ell$ converge to a normal distribution as $N\to\infty$. That is, $\sum_{\ell=1}^N\mathbf{y}_\ell - N\mathbb{E}\{\mathbf{y}_\ell\}/\sqrt{N} \xrightarrow{d} \mathcal{N}(0,\mathrm{Cov}(\mathbf{y}_\ell))$. Since both $\sum_{\ell=1}^N\mathbf{y}_\ell$ and $\mathbf{w}^A$ are Gaussian and independent of each other, the type statistics $\mathbf{T}^A$ is also asymptotically Gaussian as follows:

$$f\left(\mathbf{T}^A|\theta_i\right) \xrightarrow{d} \mathcal{N}\left(\mu_i,\Sigma_i\right), \quad \text{for } i=0,1 \quad (29)$$

where $\mu_i = N\tilde{p}_{S_i}\mu_S\tilde{\mathbf{q}}_{S_i}$ and $\Sigma_i = N\mathrm{Cov}(\mathbf{y}_\ell) + \sigma^2/(2E)\mathbf{I}$.

The next step is to characterize the error exponent with the Gaussian approximation in (29). In particular, applying the Chernoff bound with decision regions in (24) [27], we have the following asymptotic upper bound on the DEP at the ally FC:

$$\begin{aligned}P_e \le \min_{\lambda\in[0,1]} &p^\lambda(\theta_0)\,p^{1-\lambda}(\theta_1) \\ &\times\int f^\lambda\left(\mathbf{T}^A|\theta_0\right)f^{1-\lambda}\left(\mathbf{T}^A|\theta_1\right)d\mathbf{T}^A. \end{aligned} \quad (30)$$

Since $\mathbf{T}^A$ is Gaussian, the closed-form for the integral in (30) is given by [27]

$$\int f^\lambda\left(\mathbf{T}^A|\theta_0\right)f^{1-\lambda}\left(\mathbf{T}^A|\theta_1\right)d\mathbf{T}^A = e^{-k(\lambda)} \quad (31)$$

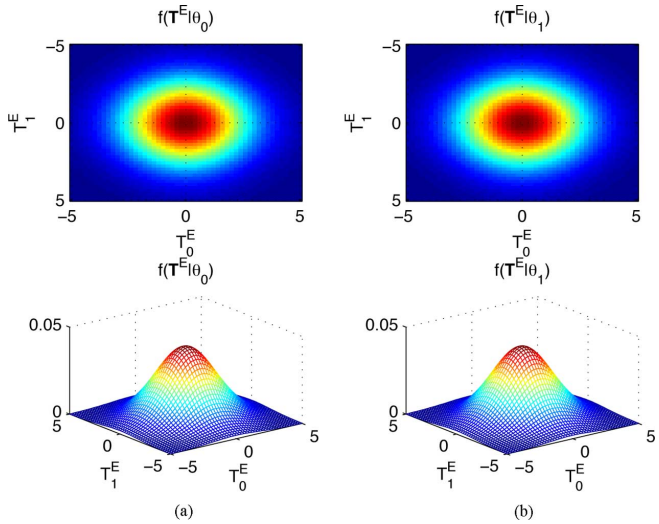

Fig. 2. Numerical results of the conditional pdfs, $f(\mathbf{T}^E|\theta_0)$ (column on the left) and $f(\mathbf{T}^E|\theta_1)$ (column on the right) for $N = 20$. The figures in the first row are contour plots of the conditional pdfs.

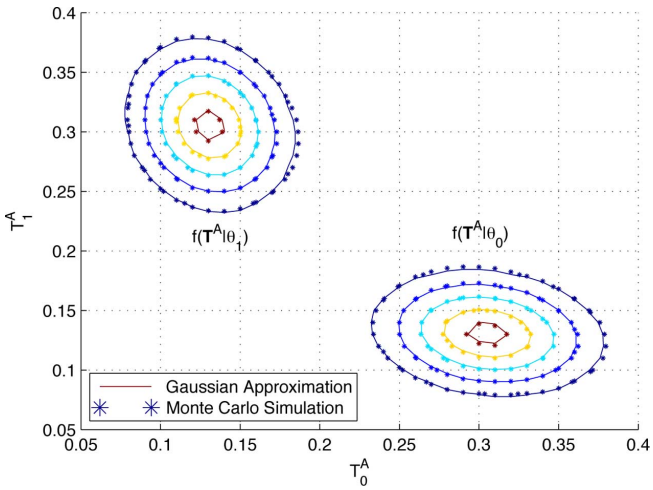

Fig. 3. Contours of the conditional pdfs, $f(\mathbf{T}^A|\theta_i)$ for $N = 500$. The solid lines indicate the analytic results from the Gaussian approximation, and the stars represent the simulation results.

where

$$k(\lambda) = \frac{\lambda(1-\lambda)}{2}(\mu_0 - \mu_1)^T \times [(1-\lambda)\Sigma_0 + \lambda\Sigma_1]^{-1}(\mu_0 - \mu_1) + \frac{1}{2}\ln\frac{\det((1-\lambda)\Sigma_0 + \lambda\Sigma_1)}{\{\det(\Sigma_0)\}^{1-\lambda}\{\det(\Sigma_1)\}^{\lambda}} \quad (32)$$

and $\det(\cdot)$ is the determinant of the matrix argument. In Section IV, we will confirm our analysis.

IV. Simulation Results

We carry out Monte Carlo simulations with the assumptions that the target states $\{\theta_0, \theta_1\}$ happen equally likely, the signal energy E at each sensor and the noise power σ^2 are normalized to 1, and each channel between a sensor and an FC has unit gain, $\mathbb{E}[|h|^2] = 1$.

We first consider a symmetric case with $p_{\theta_0}(1) = p_{\theta_1}(0) = 0.3$ for which we design the secure TBMA with $\mathbf{q}_S = \mathbf{q}_W = [1\ 1]^T$ and $p_S = p_W = 0.3$ and evaluate the conditional pdfs $f(\mathbf{T}^E|\theta_i)$ for $i = 0, 1$ and the DEP at the enemy and the ally FC, respectively. For the enemy FC, $f(\mathbf{T}^E|\theta_i)$ is numerically evaluated with $N = 20$ in Fig. 2, where we see that $f(\mathbf{T}^E|\theta_0)$ and $f(\mathbf{T}^E|\theta_1)$ look identical as intended. Thus, eavesdropping does not help the enemy FC obtain any information about the target value. The enemy FC can make a decision only by using the *a prior* probabilities of each target value, $p(\theta_0)$ and $p(\theta_1)$. In our experiment, we assume that they are equally probable; therefore, the enemy FC becomes totally ignorant of the target value.

The conditional pdfs $f(\mathbf{T}^A|\theta_i)$ for $i = 0, 1$ at the ally FC are also evaluated for $N = 500$ sensors in Fig. 3, where we compare the contours of $f(\mathbf{T}^E|\theta_i)$ obtained by the Gaussian approximation with the simulation results. It is noted that the analytic results correspond well with the simulation ones. Contrary to the conditional pdfs at the enemy FC, the results in Fig. 3 also show that the ones at the ally FC look distinct, and thus the ally FC can properly deduce the status of the target value.

To evaluate the DEP at the ally FC, we consider the secure TBMA introduced in Example 2 where the asymmetric observation channel is given by the pmfs of $\mathbf{p}_{\theta_0} = [0.4\ 0.3\ 0.2\ 0.1]^T$ and $\mathbf{p}_{\theta_1} = [0.1\ 0.2\ 0.5\ 0.2]^T$. By letting $\mathbf{q}_S = \mathbf{1}$, we present four mappings in Table II with $p_S = 0.1$ and $E/\sigma^2 = 0$ dB. Furthermore, to quantify the DEP degradation due to the interference by the sensors in $\mathcal{S}_W$, we also evaluate the DEP of the conventional (insecure) TBMA with $p_S = 0.1$ and $p_W = 0$. Fig. 4 depicts the simulation results for the DEP and the corresponding error exponents from the analysis at the ally FC for the cases with/without (or secure/insecure) the weak set $\mathcal{S}_W$. The experiment shows that the DEP of the secure TBMA decays at an exponential rate with a growing number of sensors, much like the conventional TBMA. Among the four mappings of the secure TBMA, our choice (i.e., the third row in Table II) achieves the best performance. It is also shown that the error exponents from our analysis with the Gaussian approximation in Section III-B fairly predict the exponent of the DEP of the secure TBMA. Note that the secure TBMA with the best mapping can achieve perfect secrecy at a marginal cost of DEP performance. On the contrary, the DEP at the enemy FC is 0.5 regardless of N, which is a necessary condition for perfect secrecy although a sufficient condition, $f(\mathbf{T}^E|\theta_0) = f(\mathbf{T}^E|\theta_1)$ is already achieved by following the design rule developed in Section III.

In Fig. 5, we set the number of sensors to 300 and vary p_S from 0.05 to 0.2 by a step of 0.03 to see a different view of the simulations. For each given p_S, we also change p_W to satisfy $\rho = 0.3$ or 1.0 in order to investigate the impact of the size of $\mathcal{S}_W$ on the DEP at the ally FC. The third row in Table II is used for our mapping. The simulation results show that the DEP of the secure TBMA with $\rho = 1.0$ is better than the one with $\rho = 0.3$. This result confirms our analysis in the previous section that the smaller size of $\mathcal{S}_W$ provides a better DEP. Fig. 5 also enables us to select τ_S for a target DEP at the ally FC and subsequently τ_W from the ratio $\rho = p_S/p_W$.

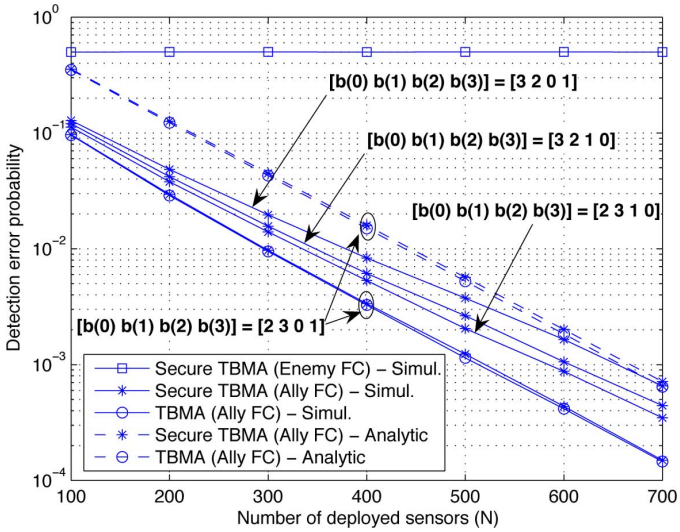

Fig. 4. Results of simulations and theoretical analysis at $p_S = 0.1$; the lines with the circles are for the conventional TBMA ($p_W = 0$), the ones with the asterisk symbols are for the secure TBMA with various mappings, and the one with the squares is the DEP of the secure TBMA at the enemy FC. All mappings in Table II are presented for comparison of the DEP.

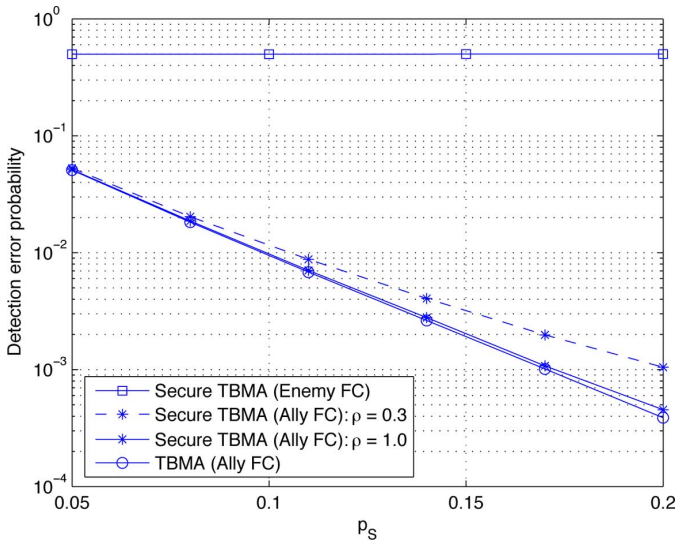

Fig. 5. DEPs of the secure TBMA over a range of p_S from 0.05 to 0.2 by a step of 0.03 when $N = 300$. The dotted and solid lines with asterisk symbols, respectively, indicate the DEPs of the secure TBMA with $\rho = 0.3$ and $\rho = 1.0$.

V. Conclusion

In this paper, we focused on data confidentiality in a distributed detection scenario with the TBMA protocol in which the wireless channels between the sensors and the ally FC are vulnerable to eavesdropping by an unauthorized enemy FC. To secure the wireless channels, we proposed a novel TBMA protocol called *secure* TBMA which provides data confidentiality by taking advantage of randomness and independence of the main and eavesdropping channels. Instead of securing the individual wireless channels based on cryptographic algorithms, the key idea behind secure TBMA is to have the activated sensors secure their transmissions from possible eavesdropping in a cooperative manner in which the sensors follow different reporting rules depending on the magnitudes of their main channel gains. It was demonstrated that the secure TBMA provides *perfect secrecy* against eavesdropping of the enemy FC.

To evaluate the level of confidentiality, we analyzed the conditional probabilities of the type statistics at the enemy FC and found relations among the design parameters to achieve perfect secrecy. In addition to the requirements for perfect secrecy, we considered energy efficiency and finally established design rules for a given observation channel. On the other hand, for the ally FC, we investigated the DEP with the Gaussian approximation to get the type statistics in a closed form. The analysis led us to a closed form expression for the error exponent of the DEP, which also provides insight into the roles of the activated sensors. The analysis demonstrated that the DEP performance loss at the ally FC is negligible since the sensors that generate interference to the ally FC are selected to have weak main channel gains, which is guaranteed by the multiuser diversity of over-deployed WSNs.

The secure TBMA delivers unconditional/perfect secrecy and, therefore, does not assume any superiority of the ally FC over the enemy FC such as secret keys known only to the ally FC and/or limits on computational capability of the enemy FC. In addition, the secure TBMA has practical advantages in that it does not count on heavy cryptographic algorithms and/or key management which are hard to implement in sensor devices with limited computing and energy resources.

The secure TBMA presented in this paper also has limits and challenges that need to be addressed in the future. First, the secure TBMA achieves perfect secrecy with more activated sensors than the ones in the conventional TBMA. The energy consumption can be reduced with power control strategies since CSI is available to the sensors, which is one of our future research topics. In addition to the energy consumption, we should elaborate more on the channel model by including non-i.i.d. communication channels, correlation between the main and eavesdropping channels, etc. Nevertheless, to the best of our knowledge, the natural resources have not been thoroughly utilized to secure the communications in the WSNs, and we believe that our work paves the way for a new study of security solutions to the WSNs.

Appendix A

For given $\mathbf{K} = [K_0, \ldots, K_{M-1}]^T$ where $K_m = N_m^S + N_m^W$, we have

$$\begin{aligned}
&\sum_{N_0^S=0}^{K_0} \cdots \sum_{N_{M-1}^S=0}^{K_{M-1}} \prod_{m=0}^{M-1} \binom{K_m}{N_m^S} [\tilde{p}_{S_i} \tilde{q}_{S_i}(m)]^{N_m^S} \\
&\qquad \times [\tilde{p}_{W_i} \tilde{q}_{W_i}(M-m-1)]^{N_m^W} \\
&= \prod_{m=0}^{M-1} \sum_{N_m^S=0}^{K_m} \binom{K_m}{N_m^S} [\tilde{p}_{S_i} \tilde{q}_{S_i}(m)]^{N_m^S} \\
&\qquad \times [\tilde{p}_{W_i} \tilde{q}_{W_i}(M-m-1)]^{N_m^W} \\
&\overset{(a)}{=} \prod_{m=0}^{M-1} [\tilde{p}_{S_0} \tilde{q}_{S_i}(m) + \tilde{p}_{W_0} \tilde{q}_{W_i}(M-m-1)]^{K_m}
\end{aligned}$$

where (a) follows from the binomial formula.

APPENDIX B

The pdf of $\tilde{\alpha}_i^A$, denoted by $f_{\tilde{\alpha}}(x)$, is derived as

$$f_{\tilde{\alpha}}(x) = \frac{f_\alpha(x)}{1 - F_\alpha(\tau_S)}, \quad \text{for } x > \tau_S$$

where $f_\alpha(x)$ and $F_\alpha(x)$ are pdf and cdf of the Rayleigh distribution, respectively. Then, the moment generating function (mgf) of $\tilde{\alpha}_i^A$ is given by

$$\begin{aligned}\varphi_1(s) &= \int_0^\infty e^{sx} f_{\tilde{\alpha}}(x)dx \\ &= \exp\left(\frac{\tau_S^2}{\sigma_h^2} + \frac{\sigma_h^2}{4}s^2\right) \\ &\quad \times \left[\exp\left(-\frac{1}{\sigma_h^2}\left(\tau_S - \frac{\sigma_h^2}{2}s\right)^2\right)\right. \\ &\quad \left. + s\sqrt{\pi\sigma_h^2}Q\left(\sqrt{\frac{2}{\sigma_h^2}}\left(\tau_S - \frac{\sigma_h^2}{2}s\right)\right)\right]\end{aligned}$$

where $Q(t) = \int_t^\infty 1/\sqrt{2\pi}e^{(-\xi^2/2)}d\xi$. Following the same way, the pdf of $\tilde{h}_j^A$ for $j \in \mathcal{S}_W$ is given by

$$f_{\tilde{h}}(x) = \left(1 - 2Q\left(\sqrt{\frac{2}{\sigma_h^2}(\tau_W^2 - x^2)}\right)\right)\frac{f_h(x)}{F_\alpha(\tau_W)}$$

where $|x| < \tau_W$ and $f_h(x)$ is the pdf of a zero-mean Gaussian random variable with variance $\sigma_h^2/2$. The mgf of $\tilde{h}_j^A$, denoted by $\varphi_2(s)$ is from a numerical integration of $\int_{-\infty}^\infty e^{sx} f_{\tilde{h}}(x)dx$ for given s.

ACKNOWLEDGMENT

The authors would like to thank D. Klinc for his comments and suggestions, which improved this manuscript.

REFERENCES

[1] I. F. Akylidiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[2] P. K. Varshney, *Distributed Detection and Data Fusion*. New York: Springer, 1997.

[3] R. Viswanathan and P. K. Varshney, "Distributed detection with multiple sensors: Part I-fundamentals," *Proc. IEEE*, vol. 85, no. 1, pp. 54–63, Jan. 1997.

[4] R. S. Blum, S. A. Kassam, and H. V. Poor, "Distributed detection with multiple sensors: Part II-advanced topics," *Proc. IEEE*, vol. 85, no. 1, pp. 64–79, Jan. 1997.

[5] J.-F. Chamberland and V. V. Veeravalli, "Decentralized detection in sensor networks," *IEEE Trans. Signal Process.*, vol. 51, no. 2, pp. 407–416, Feb. 2003.

[6] B. Chen, L. Tong, and P. K. Varshney, "Channel-aware distributed detection in wireless sensor networks," *IEEE Signal Process. Mag.*, vol. 23, no. 4, pp. 16–26, Jul. 2006.

[7] R. Niu, B. Chen, and P. K. Varshney, "Fusion of decisions transmitted over Rayleigh fading channels in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 54, no. 3, pp. 1018–1027, Mar. 2006.

[8] Q. Zhao and L. Tong, "Opportunistic carrier sensing for energy-efficient information retrieval in sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2, no. 3, pp. 231–241, Mar. 2005.

[9] Y.-R. Tsai and L.-C. Lin, "Sequential fusion for distributed detection over BSC channels in an inhomogeneous sensing environment," *IEEE Sig. Process. Lett.*, vol. 17, no. 1, pp. 99–102, Jan. 2010.

[10] C. R. Berger, M. Guerriero, S. Zhou, and P. Willett, "PAC vs. MAC for decentralized detection using noncoherent modulation," *IEEE Trans. Signal Process.*, vol. 57, no. 9, pp. 3562–3575, Sep. 2009.

[11] G. Mergen, V. Naware, and L. Tong, "Asymptotic detection performance of type-based multiple access over multiaccess fading channels," *IEEE Trans. Signal Process.*, vol. 55, no. 3, pp. 1081–1092, Mar. 2007.

[12] K. Liu and A. M. Sayeed, "Type-based decentralized detection in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 55, no. 5, pp. 1899–1910, May 2007.

[13] A. Anandkumar and L. Tong, "Type-based random access for distributed detection over multiaccess fading channels," *IEEE Trans. Signal Process.*, vol. 55, no. 10, pp. 5032–5043, Oct. 2007.

[14] K. Piotrowski, P. Langendoerfer, and S. Peter, "How public key cryptography influences wireless sensor node lifetime," in *Proc. 4th ACM Workshop on Security of ad hoc and Sensor Networks, (SASN 2006)*, Alexandria, VA, 2006, pp. 169–176.

[15] A. Perrig, J. A. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004.

[16] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, 2009.

[17] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," *Wireless Netw. J.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[18] C. Karlof, N. Sastry, and D. Wagner, Tinysec: Link Layer Security for Tiny Devices 2003 [Online]. Available: http://www.cs.berkeley.edu/Thks/tinyseC/

[19] H. Chan, A. Perrig, B. Przydatek, and D. Song, "SIA: Secure information aggregation in sensor networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 69–102, Jan. 2007.

[20] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 273–289, Jun. 2008.

[21] V. Nadendla, "Secure Distributed Detection in Wireless Sensor Networks via Encryption of Sensor Decision," M.S., Louisiana State University and Agricultural and Mechanical College, Baton Rouge, LA, 2009.

[22] G. Anastasi, M. Conti, M. Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, May 2009.

[23] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[24] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[25] T. Cover and J. Thomas, *Elements of Information Theory*, 1st ed. Hoboken, NJ: Wiley, 1991.

[26] P. Billingsley, *Probability and Measure*. New York: Wiley Inter-Sci, 1995.

[27] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*. New York: Wiley Inter-Sci, 2001.

Hyoungsuk Jeon (S'07–M'11) received the B.S. degree in electrical engineering from Dongguk University, Seoul, Korea in 2004, and the M.S. and Ph.D. degrees in information and communications engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2005 and 2010, respectively.

Since September 2010, he has been with electrical engineering in KAIST as a postdoctoral researcher. He is currently a visiting faculty member at Georgia Institute of Technology, Atlanta, GA, from December 2010 to the present. His research interests are in the fields of communications, signal processing, and information theory, especially design and analysis of distributed detection and physical layer security.

Daesung Hwang (S'08) received the B.S. and M.S. degrees in electrical engineering from Information and Communications University, and Korea Advanced Instituted of Science and Technology (KAIST), Daejeon, Korea, in 2008 and 2010, respectively. He is working toward the Ph.D. degree in electrical engineering at KAIST.

His research interests include the distributed schemes in sensor networks.

Jinho Choi (S'89–M'91–SM'02) was born in Seoul, Korea. He received the B.E. (*magna cum laude*) degree in electronics engineering in 1989 from Sogang University, Seoul, and the M.S.E. and Ph.D. degrees in electrical engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 1991 and 1994, respectively.

He is now with the School of Engineering, Swansea University, U.K., as a Professor/Chair of Wireless. His research interests include wireless communications and array/statistical signal processing. He authored two books published by Cambridge University Press in 2006 and 2010.

Prof. Choi received the 1999 Best Paper Award for Signal Processing from EURASIP, and the 2009 Best Paper Award from WPMC (Conference). Currently, he is an Editor of the *Journal of Communications and Networks* (JCN) since 2005 and served as an Associate Editor of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2005 to 2007 and the *ETRI Journal*. In 2009, he joined the Editorial Board of *International Journal of Vehicular Technology*.

Hyuckjae Lee (S'76–M'81) was born in Incheon, Korea. He received the B.S. degree in electronic engineering from Seoul National University, Seoul, Korea, in 1970, and the M.S. and Ph.D. degrees in electrical engineering from Oregon State University, Corvallis, in 1977 and 1982, respectively.

From 1983 to 2000, he was with the Radio Technology Department, Electronics and Telecommunications Research Institute (ETRI), and worked in the fields of radio technology, IMT-2000, broadcasting technology, and satellite communication systems. In 2000, he joined Information and Communications University (ICU), Daejeon, Korea, as a professor. In 2002, he set up the radio education and research center in ICU to enhance the quality of undergraduate education of radio-related fields. Since 2005, he has served as a chairman of the Mobile RFID Forum in Korea. He is currently a professor of Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea.

Jeongseok Ha (M'06) received the B.E. degree in electronics from Kyungpook National University, Daegu, Korea in 1992, the M.S. degree in electronic and electrical engineering from Pohang University of Science and Technology, Pohang, Korea, in 1994, and the Ph.D. degree in electrical and computer engineering from Georgia Institute of Technology, Atlanta, in 2003.

He is now with Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, as an associate professor. His research interests include theories and applications of error-control codes and physical layer security.