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/JIOT.2018.2842056, IEEE Internet of Things Journal

Exploiting Mapping Diversity for Enhancing Security at Physical Layer in the Internet of Things

Sasi Vinay Pechetti, *Student Member, IEEE,* Abhishek Jindal, *Member, IEEE,*

and Ranjan Bose, *Senior Member, IEEE*

***Abstract*—Application of internet of things (IoT) in health, defense, banking and other confidential information transfer urges the need for secure IoT. As most of the IoT devices are resource-limited (antennas, bandwidth, energy), securing the information transfer has always been a challenge. Looking at a solution for enhancing the security of single antenna, single carrier, energy efficient devices, we propose a novel scheme, channel-based mapping diversity (CBMD). This scheme uses the inherent randomness of the wireless channel and multiple mappings available for an M-ary phase shift keying (M-PSK) constellation in confusing an eavesdropper. When the legitimate and the eavesdropper channels are independent of each other, it is shown that a symbol error rate (SER) of $\frac{M-1}{M}$ is induced at the eavesdropper. Whereas, when the channels are correlated, optimal and sub-optimal strategies at source and eavesdropper are derived for their respective optimal performances. Further, a closed-form expression for a lower-bound on the SER at the eavesdropper is derived. Simulation results show that for the correlated case, as SNR at the eavesdropper increases, SER initially decreases, later saturates to a relatively high SER, hence making the job of the eavesdropper difficult in getting the legitimate data. Furthermore, the effect of the correlation is more pronounced on SER at higher levels of correlation. This indicates that for practical correlation scenarios, SER is high enough to confuse the eavesdropper.**

***Index Terms*—IoT, SER, diversity, physical layer security, correlated eavesdropper.**

I. Introduction

A. Motivation

Broadcasting through wireless medium has made the information transfer vulnerable to eavesdropping. This makes secure information transfer on wireless medium challenging. A conventional way that is followed to secure the information transfer is to use techniques based on cryptography. But these techniques are known to be computationally hungry and have high latency due to the exchange of secret key [3]. In order to overcome these, physical layer security (PLS) techniques have been proposed which take advantage of random characteristics of the channel. [4], [5] are a few among the pioneers in PLS to show that the information transfer can indeed be perfectly secure. Recently, after the emergence of multiple antenna techniques, PLS has gained more attention than ever before [6]. Authors in [7] have shown that even in the absence of eavesdropper's channel state information (CSI), a positive secrecy is achieved. In their work, transmitter having multiple antennas transmit the legitimate signal along with a random artificial noise, where the artificial noise is designed such that it is nulled at the legitimate receiver. Authors in [8] have improved secrecy of a source-destination link using relays and jammers with the help of artificial noise. X. Li *et.al*. in [9], have exploited the redundancy of transmit antennas to create an artificial fading at the eavesdropper, hence improving the secrecy. Several related works can be found in [6], which try to secure the information transfer. More recently, authors in [10] have analyzed secrecy outage using cooperative jamming for enhancing PLS in IoT. These conventional information-theoretic based physical layer techniques trying to maintain positive secrecy of the system mostly requires either the CSI of the adversary or extra resources like artificial noise along with multiple antennas, multiple sub-carriers etc. Even though, these information-theoretic techniques provide perfect secrecy, the extra resources used are not always affordable by all devices, especially, when it comes to platforms like IoT [11]. Therefore, for the devices which cannot afford multiple antennas, multiple sub-carriers, artificial noise etc, enforces the need of low cost, less complex techniques. To this end, a few signal-processing techniques dealing with SER are proposed, which make the job difficult at the adversary are discussed in [11] and references therein.

In this context, authors in [12] have proposed a constellation diversity technique, where they select a particular constellation for modulating the data and transmit it over an additive white Gaussian noise (AWGN) channel. Source selects either a circular or a rectangular quadrature amplitude modulation, each time when data has to be transmitted. Selection of a constellation is done based on a pre-shared key known only to the legitimate parties, thereby, inducing the maximum SER at the adversary. However, one major drawback with this method is that if the key is not long enough, eavesdropper can apply advanced blind constellation techniques to estimate the constellation shape, thereby, decoding the data. In addition, exchanging a pre-shared key securely is also an issue. One of the most recent signal processing techniques dealing with SER in this line is proposed in [13], where the authors use the concept of directional modulation in forming the desired symbol at the receiver rather than transmitting the symbol at the transmitter. Thereby, making the adversary almost

S. V. Pechetti, R. Bose are with the Dept. of Electrical Engg., and A. Jindal was with the Bharti School of Telecomm. Tech. & Mgmt. at Indian Institute of Technology Delhi, Delhi-110016, India. A. Jindal is now with UT Dallas, Richardson, US (email: eez158097@ee.iitd.ac.in, abjindal11@gmail.com and rbose@ee.iitd.ernet.in). A part of this work was presented at the *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* [1] and filed in [2].

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/JIOT.2018.2842056, IEEE Internet of Things Journal

impossible to guess the symbol that was transmitted at the source, hence inducing the maximum SER at the adversary. Looking from multi-carrier perspective, [14], [15] have made use of orthogonal sub-carriers undergoing independent fading to confuse the adversary. Interleaving of the data that is to be transmitted on each sub-carrier is done based on the magnitude of the channels gains of each sub-carrier, which are assumed to be available at both the legitimate nodes.

More recently, authors in [16] have proposed a spoofing technique for binary-PSK (BPSK) and quadrature-PSK (QPSK) in deteriorating the performance at the malicious receiver in an AWGN scenario. In the paper, they have used an extra friendly spoofing node which changes the received symbol at the malicious receiver. H. Jeon et.al in [17], [18] have proposed a channel aware encryption technique to secure the information transfer from sensors to a fusion center in a wireless sensor network scenario. It is assumed that the channel from each sensor to the fusion center is known to the respective sensor. This channel gain, when compared to a threshold, is used to select one of the two available non-coherent orthogonal frequencies for transmitting the data. In other words, based on the channel gain, sensor does a bit flipping operation on the data that is to be transmitted. They show that as the number of sensors grow larger, it is possible to achieve perfect secrecy assuming that the channel from the sensor to the ally fusion center is independently fading with the channel from the sensor to the eavesdropping fusion center.

Although, most of the techniques discussed above use diverse nature of multiple antennas, multiple sub-carriers, multiple nodes, these are less complex when compared to conventional information theoretic techniques [11]. In our previous work [1], we have proposed CBMD as a solution for point-to-point, single-antenna, single-carrier communication for BPSK modulation.

In this, a mapping is chosen from two available mappings of a BPSK constellation for data transmission based on the channel gain. A bit error rate (BER) of 0.5 is induced at the eavesdropper when the source (S) to destination (D) channel is independently fading with respect to (w.r.t.) source to eavesdropper (E) channel. Further, when the legitimate ($S-D$) and the eavesdropper ($S-E$) channels are correlated, optimal thresholds were derived for BPSK constellation.

However, due to the demand of larger data rate, a similar scheme based on the mapping diversity for higher order modulations like $M-$PSK is required, which is proposed in the present paper. Working on the non-trivial extension of [1], we propose a novel way to select an appropriate set of mappings and the mapping strategy for the selected set. Further, we have solved the complicated problem of deriving the optimal strategies for respective optimal performances of source and eavesdropper. Taking a step further, we have derived a closed-form lower bound on the SER. Major contributions of this work are explicitly listed below in more detail.

B. Major Contributions

1. (a) We select a mapping for data transmission based on the legitimate channel gain. Unlike in BPSK [1], which just has 2! $(= 2)$ possible mappings for a given constellation shape, $M-$PSK has $M!$ possible mappings. We propose a method for choosing an appropriate set, out of which a mapping is selected each time when data is transmitted.
   (b) After choosing an appropriate set, we design a threshold-based selection strategy for selecting a particular mapping based on the legitimate channel gain. It is also ensured that the mapping selection strategy has the least effect on destination's performance.
2. (a) When the legitimate and the eavesdropper channels are independent of each other, for an appropriately chosen threshold, we show that an SER of $\frac{M-1}{M}$ is induced at E.
   (b) We propose methods for choosing the thresholds at E and S for their optimal performances respectively.
3. Since obtaining a closed-form expression for SER is difficult, a closed-form lower-bound on the SER at E for various modulation orders are derived.
4. We obtain a sub-optimal threshold based on the median of the square of legitimate channel gain which performs very close to the optimal threshold.

C. Organization

The rest of the paper is organized as the following: System model is discussed in Section II. In Section III, CBMD is discussed along with a detailed discussion on mapping selection strategy. Error analysis for both independent and correlated channel cases are done in Section IV. Section V briefly discusses the bounds derived on the SER at E. Later, simulation results validating the analysis are presented in Section VII. Finally, we conclude our work with a few notable points and future directions in Section VIII.

Notation: Any subscript and superscript greater than M is reduced by the $modulo(M)$ operation throughout the paper.

II. System Model

In this paper, we consider a simple system model consisting of an E trying to tap the information transfer between S and D. All nodes are considered to be single antenna nodes. During the first phase, S transmits the pilot signal, while D and E estimate their respective channels $S-D$ and $S-E$. Similarly, during the second phase, D transmits the pilot signal, while S and E estimate their respective channels $D-S$ and $D-E$. Channel between S and D is assumed to be reciprocal, hence links $S-D$ and $D-S$ are identical. Further, we assume that E is at least separated by a distance of half the wavelength from D. Therefore, the channels estimated at E in the first phase and the second phase of piloting ($S-E$ and $D-E$) are different from the legitimate channel ($S-D$). Hence, S and D have the knowledge of the channel $S-D$, while E has the knowledge of the channels $S-E$ and $D-E$. Perfect CSI of the legitimate channel is assumed to be available at S and D, however, in later part of the paper, imperfect CSI is considered and has been dealt with.

Channels $S-D$ and $S-E$ are both considered to be quasi-static Rayleigh block fading with channel coefficients $h_M \sim$

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/JIOT.2018.2842056, IEEE Internet of Things Journal

$\mathcal{CN}(0, \frac{1}{\lambda_S})$ and $h_E \sim \mathcal{CN}(0, \frac{1}{\lambda_E})$ respectively. The received signals at D and E are given respectively as:

$$r_D = h_M s + n_D, \quad r_E = h_E s + n_E, \tag{1}$$

where s is the transmitted symbol, and n_D, n_E are additive white Gaussian noises at D, E respectively with mean zero and variance N_0. We further denote,

$$x = |h_E|^2 \quad \text{and} \quad y = |h_M|^2, \tag{2}$$

as two exponential random variables with means $\frac{1}{\lambda_S}$ and $\frac{1}{\lambda_E}$ respectively derived from the statistics of h_M and h_E.

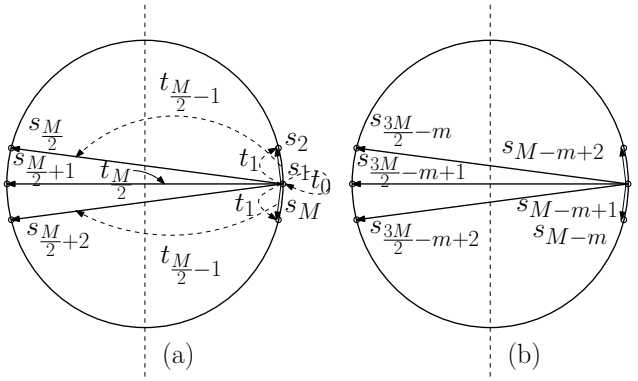
III. Channel-based mapping diversity (CBMD)

In this section, we propose a scheme, channel-based mapping diversity, which uses different possible mappings of an M-PSK constellation along with the CSI of the main channel for confusing E. The basic idea is to choose a mapping from a finite set of mappings that are available for an M-PSK constellation for data transmission based on the value of y.

A. Selection of Set of Mappings

As the data is assumed to be uniformly distributed, in the worst case, E can keep guessing a fixed symbol every time when a signal is received, thereby, achieving the maximum SER $\frac{M-1}{M}$. Since there are M possible symbols that are to be mapped to M possible constellation points, there can be in total $M!$ possible mappings for an M-PSK constellation, out of which we need to choose a subset such that an SER of $\frac{M-1}{M}$ is induced at E. However, choosing a set with larger cardinality increases the computational complexity at S and D. Therefore, we choose a set such that the maximum SER is induced at E with minimum cardinality. Moreover, the chosen set should contain Gray mappings so that there is no compromise on the performance at D.

Say, for instance if we choose a set having less than M mappings then it can be clearly observed that each constellation point of M-PSK cannot be occupied by every possible symbol. Therefore, when E is guessing a fixed symbol, inducing an SER of $\frac{M-1}{M}$ is not always possible. Hence, the minimum cardinality of the set is at least M. Let us consider a conventional Gray mapping of an M-PSK constellation given in Fig. 1(a), where, $s_1,\ s_2, \ldots, s_M$ are all possible symbols of an M-PSK constellation and $t_1, \ldots, t_{\frac{M}{2}}$ are the probabilities of errors that are to be induced by the channel for converting one symbol into its 1^{st}, 2^{nd}, $\ldots$, $\frac{M}{2}^{th}$ adjacent symbols at the receiver respectively. Now, the set $\mathbb{S}$ consisting of rotated versions of this conventional Gray mapping, shown in Fig. 1(b), with phases $\theta = \frac{2m\pi}{M},\ m \in \{0, 1, \ldots, M-1\}$ has M mappings, all of which are Gray. In addition, every constellation point is occupied by every possible symbol, hence making it possible to induce an error of $\frac{M-1}{M}$. There can be many other sets possible which can induce the maximum SER, but the set $\mathbb{S}$ has the minimum cardinality. An example of the set $\mathbb{S}$ for 8-PSK is shown in Fig. 3. Now that we have arrived at a set of mappings, choosing one of the mapping from the set $\mathbb{S}$ each time when data is to be transmitted based on the main channel gain is discussed in the following section.



Conventional M-PSK Mapping m^{th} rotation of conventional mapping

Fig. 1: Selected set of Gray mappings for $M-$PSK constellation. Every subscript is taken $modulo(M)$.

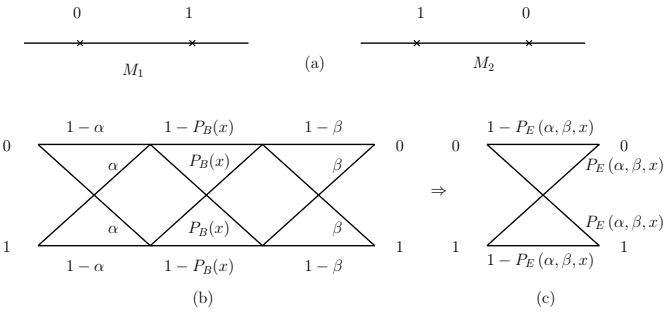


Fig. 2: (a) Possible mappings for BPSK. (b) Effective channel for E with CBMD. (c) Equivalent BSC for CBMD.

B. Channel-based mapping selection strategy

In this section, for the better understanding of the scheme, we first briefly discuss the strategy for BPSK presented in [1], and later we study the case of $M-$PSK.

1) Mapping selection strategy for BPSK (2-PSK): BPSK has two possible mappings M_1 and M_2, for a given constellation shape shown in Fig. 2(a), where S selects one of them each time when data is transmitted. Let τ_S be the threshold at S, where it switches its mapping, i.e., if $y \leq \tau_S$, S selects M_1, otherwise it selects M_2. Further, let τ_E be the threshold at E. This selection can be mathematically represented using Bernoulli random variables, α, β related to y and x respectively as,

$$\alpha = \begin{cases} 0 & y \leq \tau_S \\ 1 & y > \tau_S \end{cases}, \ \beta = \begin{cases} 0 & x \leq \tau_E \\ 1 & x > \tau_E \end{cases}. \tag{3}$$

As, it is assumed that perfect CSI is available at S and D, there will be no induced error due to CBMD at D. Therefore, the cross over probability in converting '0' to '1' or '1' to '0' at the receiver due to the error induced by the channel is given by [19],

$$P_B(y) = Q\left(\sqrt{cy}\right), \qquad c = \frac{2P_S}{N_0}, \tag{4}$$

where $Q(.)$ is the Gaussian Q-function and P_S is the transmit power at S. However, at E, there will be an error induced by CBMD due to the mismatch in the mapping selected. Using

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/JIOT.2018.2842056, IEEE Internet of Things Journal

the formulation given in (3), the effective channel of $S-E$ can be visualized as in Fig. 2(b), consisting of three cascaded binary symmetric channels (BSCs). Where the first BSC in the Fig. 2(b), with cross over probability α is representing the mapping selection at the source, i.e, if $\alpha=0$, mapping M_1 is chosen, else if $\alpha=1$, mapping M_2 is chosen for data transmission. The second BSC in the Fig. 2(b), with cross over probability $P_B(x)$, represents the probability of in converting '0' to '1' or '1' to '0' due to the error induced by the eavesdropper's channel. The third BSC in Fig. 2(b), with cross over probability β, represents the mapping selection at the eavesdropper, i.e, if $\beta=0$, mapping M_1 is chosen, else if $\beta=1$, mapping M_2 is chosen for decoding. Using the basic information and probability theory, Fig. 2(b) can be simplified as Fig. 2(c), where the effective cross-over probability of the eavesdropper's channel is given by,

$$\begin{aligned} P_E^{BPSK}(\alpha,\beta,x) =& P_B(x)\left[1+4\alpha\beta-2(\alpha+\beta)\right] \\ &+\left[(\alpha+\beta)-2\alpha\beta\right]. \end{aligned} \tag{5}$$

Unlike in BPSK [1], the selection of a mapping based on the channel gain and its error probability analysis is bit more involved and is discussed in the following.

2) Mapping selection strategy for M-PSK: Motivated by the strategy for BPSK, we propose a strategy for $M-$PSK based on the legitimate channel gain. In M-PSK, selecting each one of the M mappings from the set $\mathbb{S}$ need M decision regions based on the legitimate channel gain y. One simple extension is to consider $\log_2 M$ consecutive independent channel fading blocks for designing $\log_2 M$ independent Bernoulli random variables. Hence, forming $2^{\log_2 M}=M$ decision regions for selecting each mapping from the set $\mathbb{S}$. This is mathematically represented as,

$$\begin{aligned} \alpha_{i-j}=\begin{cases} 0 & y(j)\le\tau_S(j) \\ 1 & y(j)>\tau_S(j) \end{cases},\ \beta_{i-j}=\begin{cases} 0 & x(j)\le\tau_E(j) \\ 1 & x(j)>\tau_E(j) \end{cases}. \\ \forall j\in\{i,(i-1),\ldots,(i+1-\log_2 M)\}, \end{aligned} \tag{6}$$

where i is the index of the current channel block of transmission, and $j\in\{i,(i-1),\ldots,(i-\log_2 M+1)\}$ are the indices of $\log_2 M$ consecutive independent previous channel blocks. $\alpha_{(i-j)}$ and $\beta_{(i-j)}$ are the Bernoulli random variables corresponding to the j^{th} main channel gain $y(j)$ and j^{th} eavesdropper channel gain $x(j)$ respectively. Further, $\tau_S(j)$ and $\tau_E(j)$ are the thresholds at S and E respectively. Since each channel block varies independently, $\alpha_0,\alpha_1,\ldots,\alpha_{(\log_2 M-1)}$ all are independent. Similarly $\beta_0,\beta_1,\ldots,\beta_{(\log_2 M-1)}$ are independent. Therefore, using these $\log_2 M$ independent Bernoulli random variables $\alpha_{(i-j)}$, $2^{\log_2 M}=M$ decision regions can be formed. Depending on the values of $\alpha_{(i-j)}$ and $\beta_{(i-j)}$, mappings can be selected for encoding at S and for decoding at E respectively. For example, in 8-PSK, for selecting each one of the mapping from the set $\mathbb{S}$ given in Fig. 3, we need $\log_2 M=\log_2 8=3$ consecutive channel blocks for forming eight decision regions, with $j\in\{i,i-1,i-2\}$. Now, $y(j)$ is compared with its threshold $\tau_S(j)$, hence, generating 8 exclusive regions as shown in Table I, where the fourth column

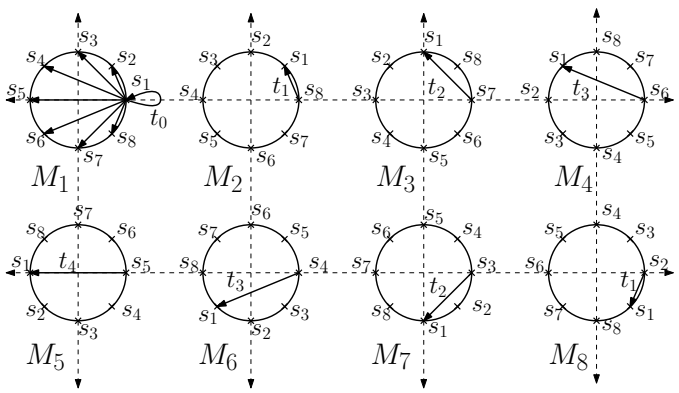


Fig. 3: Selected Set of Gray Mappings for $8-$PSK

of Table I is given by,

$$A=g(\alpha_2)g(\alpha_1)g(\alpha_0),\ g(\alpha_{(.)})\in\{\alpha_{(.)},\overline{\alpha}_{(.)}\}, \tag{7}$$

where $\overline{\alpha}_{(.)}=1-\alpha_{(.)}$. Since the regions described by each row of Table I are mutually exclusive, according to the formulation in (6), 'A' is non-zero in one row and zero in rest of the rows. The mapping corresponding to the nonzero row of 'A' is chosen at S to transmit the data. It can be seen that the mapping assignment is Gray coded. Therefore, if there is an error in channel estimation either at S and/or D then the mapping mismatch caused at S and D will have minimal impact on the performance at D. A similar mapping assignment table can be designed for an M-PSK constellation.

For analyzing symbol error at E, a similar table can be designed with parameters $x(j)$, $\tau_E(j)$ and β_{i-j}. For example, in $8-$PSK, consider a case where mapping M_1 is selected by S to transmit a data symbol s_1, then the received signal at E is correctly decoded only if,

- E chooses M_1 and there is no error induced (t_0 as shown in Fig. 3, M_1 mapping) by E's channel or
- M_2 is chosen by E and the error induced (t_1 as shown in Fig. 3 M_2 mapping) by E's channel converts s_8 to s_1,
- M_3 is chosen by E and the error induced (t_2 as shown in Fig. 3 M_3 mapping) by E's channel converts s_7 in to s_1 and so on...,
- M_8 is chosen at E and the error induced (t_1 as shown in Fig. 3 M_8 mapping) by E's channel converts s_2 to s_1.

All other cases yield in a symbol error at E when s_1 is

TABLE I: Mapping selection for 8-PSK based on legitimate channel gain $y_{(.)}$

$y(i)$	$y(i-1)$	$y(i-2)$	A	M
$>\tau_S(i)$	$>\tau_S(i-1)$	$>\tau_S(i-2)$	$\alpha_2\alpha_1\alpha_0$	M_1
$>\tau_S(i)$	$>\tau_S(i-1)$	$\le\tau_S(i-2)$	$\alpha_2\alpha_1\overline{\alpha_0}$	M_2
$>\tau_S(i)$	$\le\tau_S(i-1)$	$\le\tau_S(i-2)$	$\alpha_2\overline{\alpha_1}\alpha_0$	M_3
$>\tau_S(i)$	$\le\tau_S(i-1)$	$>\tau_S(i-2)$	$\alpha_2\overline{\alpha_1}\alpha_0$	M_4
$\le\tau_S(i)$	$\le\tau_S(i-1)$	$>\tau_S(i-2)$	$\overline{\alpha_2}\alpha_1\alpha_0$	M_5
$\le\tau_S(i)$	$\le\tau_S(i-1)$	$\le\tau_S(i-2)$	$\overline{\alpha_2}\alpha_1\alpha_0$	M_6
$\le\tau_S(i)$	$>\tau_S(i-1)$	$\le\tau_S(i-2)$	$\overline{\alpha_2}\alpha_1\overline{\alpha_0}$	M_7
$\le\tau_S(i)$	$>\tau_S(i-1)$	$>\tau_S(i-2)$	$\overline{\alpha_2}\alpha_1\alpha_0$	M_8

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/JIOT.2018.2842056, IEEE Internet of Things Journal

TABLE II: Probability of errors by the eavesdropper's channel so that the transmitted symbol is correctly decoded at E.

Mapping selected $\downarrow S \setminus E \rightarrow$	M_1 $\beta_2\beta_1\beta_0$	M_2 $\beta_2\beta_1\overline{\beta_0}$	M_3 $\beta_2\overline{\beta_1}\beta_0$	M_4 $\beta_2\overline{\beta_1}\overline{\beta_0}$	M_5 $\overline{\beta_2}\beta_1\beta_0$	M_6 $\overline{\beta_2}\beta_1\overline{\beta_0}$	M_7 $\overline{\beta_2}\overline{\beta_1}\beta_0$	M_8 $\overline{\beta_2}\overline{\beta_1}\overline{\beta_0}$
M_1 $\alpha_2\alpha_1\alpha_0$	t_0	t_1	t_2	t_3	t_4	t_3	t_2	t_1
M_2 $\alpha_2\alpha_1\overline{\alpha_0}$	t_1	t_0	t_1	t_2	t_3	t_4	t_3	t_2
M_3 $\alpha_2\overline{\alpha_1}\alpha_0$	t_2	t_1	t_0	t_1	t_2	t_3	t_4	t_3
M_4 $\alpha_2\overline{\alpha_1}\overline{\alpha_0}$	t_3	t_2	t_1	t_0	t_1	t_2	t_3	t_4
M_5 $\overline{\alpha_2}\alpha_1\alpha_0$	t_4	t_3	t_2	t_1	t_0	t_1	t_2	t_3
M_6 $\overline{\alpha_2}\alpha_1\overline{\alpha_0}$	t_3	t_4	t_3	t_2	t_1	t_0	t_1	t_2
M_7 $\overline{\alpha_2}\overline{\alpha_1}\alpha_0$	t_2	t_3	t_4	t_3	t_2	t_1	t_0	t_1
M_8 $\overline{\alpha_2}\overline{\alpha_1}\overline{\alpha_0}$	t_1	t_2	t_3	t_4	t_3	t_2	t_1	t_0

transmitted using mapping M_1. Since the error introduced by the channel depends only on the current channel, t_k, $k \in \{0, 1...\frac{M}{2}\}$ is a function of current channel block $x(i)$ alone (for details, see Appendix-E), henceforth, it is represented as t_k^i. It should be noted that for $k > \frac{M}{2}$, $t_k^i = t_{M-k}^i$. Various cases where various symbols are correctly decoded are given in Table II. Here, the first column represents the mapping chosen at S and the first row represents the mapping chosen at E. Each element of the Table II, say, $q_{m_1 m_2}$, represents the probability of error that is to be induced by the eavesdropper's channel when M_{m_1} is chosen at S and M_{m_2} is chosen at E such that the transmitted symbol is decoded correctly at E. Since the received signal has to be in one of the decision regions, from Figs. 3 and 1, we have,

$$t_0^i + t_{\frac{M}{2}}^i + 2\sum_{k=1}^{\frac{M}{2}-1} t_k^i \;=\; 1. \tag{8}$$

The probability of symbol error at E is given by,

$$P_E = 1 - P_C, \tag{9}$$

where P_C is the probability of correct decoding. Let $\Pr(M_{m_1}^E M_{m_2}^S)$ be the probability of choosing the mappings $M_{m_1}^E$ and $M_{m_2}^S$ at S and E respectively. Then P_C is given from the Table II as,

$$\begin{aligned} P_C &= t_0^i \Pr(M_1^E M_1^S) + \cdots + t_{\frac{M}{2}-1}^i \Pr(M_1^E M_{\frac{M}{2}}^S) \\ &\quad + t_{\frac{M}{2}}^i \Pr(M_1^E M_{\frac{M}{2}+1}^S) + \cdots + t_1^i \Pr(M_1^E M_M^S) \dots \\ &\quad + t_1^i \Pr(M_M^E M_1^S) + \cdots + t_{\frac{M}{2}}^i \Pr(M_M^E M_{\frac{M}{2}}^S) \\ &\quad + t_{\frac{M}{2}-1}^i \Pr(M_M^E M_{\frac{M}{2}+1}^S) + \cdots + t_0^i \Pr(M_M^E M_M^S) \\ &= \sum_{m_1=1}^{M} \sum_{m_2=1}^{M} t_{|m_1-m_2|}^i \Pr(M_{m_2}^E M_{m_1}^S). \end{aligned} \tag{10}$$

Now, collecting terms with the same subscript for $t_{(.)}^i$ together, and using $t_k^i = t_{M-k}^i$, $for\ k > \frac{M}{2}$, we get,

$$\begin{aligned} P_C &= t_0^i \sum_{m=1}^{M} \Pr(M_m^E M_m^S) + t_{\frac{M}{2}}^i \sum_{m=1}^{M} \Pr(M_m^E M_{\frac{M}{2}+m}^S) \\ &+ t_1^i \sum_{m=1}^{M} \Big[\Pr(M_m^E M_{m+1}^S) + \Pr(M_m^E M_{M+m-1}^S)\Big] \dots \\ &+ t_{\frac{M}{2}-1}^i \sum_{m=1}^{M} \Big[\Pr(M_m^E M_{m+\frac{M}{2}-1}^S + \Pr(M_m^E M_{\frac{M}{2}+1+m}^S)\Big], \end{aligned} \tag{11}$$

Now, for $M = 2$, the probability of correctness boils down to,

$$\begin{aligned} P_C^{M=2} &= t_0^i \sum_{m=1}^{2} \Pr(M_m^E M_m^S) + t_1^i \sum_{m=1}^{2} \Pr(M_m^E M_{1+m}^S) \\ &= t_0^i [\Pr(M_1^E M_1^S) + Pr(M_2^E M_2^S)] \\ &\quad + t_1^i [\Pr(M_1^E M_2^S) + Pr(M_2^E M_1^S)]. \end{aligned} \tag{12}$$

Following the formulation in (6), (8) and Table II, we get,

$$\begin{aligned} P_C^{M=2} &= (1 - t_1^i)[\alpha_0\beta_0 + \overline{\alpha_0}\overline{\beta_0}] + t_1[\alpha_0\overline{\beta_0} + \overline{\alpha_0}\beta_0] \\ &= t_1^i[2(\alpha_0 + \beta_0) - 4\alpha_0\beta_0 - 1] + [1 + 2\alpha_0\beta_0 - \alpha_0. - \beta_0] \end{aligned} \tag{13}$$

Therefore, the probability of error for BPSK ($M = 2$) is,

$$\begin{aligned} P_E^{M=2} &= 1 - P_C^{M=2} \\ &= t_1^i[1 + 4\alpha_0\beta_0 - 2(\alpha_0 + \beta_0)] + [\alpha_0 + \beta_0 - 2\alpha_0\beta_0], \end{aligned} \tag{14}$$

which is same as shown in (5), where $t_1^i = P_B(x)$. Now, to maximize the confusion at E, we next try to maximize the SER at E by designing appropriate thresholds $\tau_S(j)$, $j \in \{i+1-\log_2 M, \dots, i\}$ at S, which is discussed in the following section.

IV. Performance Analysis

In this section, we analyze the SER at E of the proposed CBMD for the following two cases, when the channels $S-D$ and $S-E$ are (i) independent, (ii) correlated. Also, we analyze the effect of imperfect CSI on the destination's performance.

A. SER at E-Independent Channels

Proposition 1. *The optimal threshold τ_S^{opt} chosen at S, which induces an SER of $\frac{M-1}{M}$ at E, is given as,*

$$\tau_S^{opt} = \tau_S^{Median} = \frac{\ln 2}{\lambda_S}. \tag{15}$$

Proof. SER at E is given by $\overline{P}_E = 1 - \overline{P}_C$, where from (11), $\overline{P}_C$ is given as,

$$= \mathbb{E}\left[t_0^i \sum_{m=1}^{M} \Pr(M_m^E M_m^S) + t_{\frac{M}{2}}^i \sum_{m=1}^{M} \Pr(M_m^E M_{\frac{M}{2}+m}^S) \right]$$

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/JIOT.2018.2842056, IEEE Internet of Things Journal

$$+\mathbb{E}\left[t_1^i \sum_{m=1}^{M}\left[\Pr(M_m^E M_{m+1}^S)+\Pr(M_m^E M_{M+m-1}^S)\right]\right]\cdots \tag{16}$$

$$+\mathbb{E}\left[t_{\frac{M}{2}-1}^i \sum_{m=1}^{M}\left[\Pr(M_m^E M_{m+\frac{M}{2}-1}^S)+\Pr(M_m^E M_{\frac{M}{2}+1+m}^S)\right]\right]$$

Since, the channels are independent, $y(.)$ and $x(.)$ are independent, therefore, $\alpha_{(.)}$ is independent of $x(.)$ and $\beta_{(.)}$. Hence,

$$\mathbb{E}\left[t_{(.)}^i \Pr(M_{m_2}^E M_{m_1}^S)\right]=\mathbb{E}\left[t_{(.)}^i \Pr(M_{m_2}^E)\right]\mathbb{E}\left[\Pr(M_{m_1}^S)\right]. \tag{17}$$

Assuming all the mappings are equally probable, $\Pr(M_{\hat{m}}^S = M_m^S)=\frac{1}{M}, \forall\ \hat{m}$, substituting (17) in (16), we get,

$$\begin{aligned}\overline{P}_C=\frac{1}{M}\Bigg\{&\mathbb{E}\left[t_0^i\sum_{m=1}^{M}\Pr(M_m^E)\right]+\mathbb{E}\left[t_{\frac{M}{2}}^i\sum_{m=1}^{M}\Pr(M_m^E)\right]\\&+\mathbb{E}\left[t_1^i\left[\sum_{m=1}^{M}\Pr(M_m^E)+\sum_{m=1}^{M}\Pr(M_m^E)\right]\right]\cdots\\&+\mathbb{E}\left[t_{\frac{M}{2}-1}^i\left[\sum_{m=1}^{M}\Pr(M_m^E)+\sum_{m=1}^{M}\Pr(M_m^E)\right]\right]\Bigg\}.\end{aligned} \tag{18}$$

Since, the received symbol belongs to one of the M mappings, we have, $\sum_m^M \Pr(M_m^E)=1$. Therefore, using (8), we get,

$$\overline{P}_C=\frac{1}{M}\times\mathbb{E}\left[t_0^i+t_{\frac{M}{2}}^i+2\sum_{m=1}^{\frac{M}{2}-1}t_m^i\right]=\frac{1}{M}. \tag{19}$$

Hence, the SER for M-PSK at E is given by,

$$\overline{P}_E^{M-PSK}=1-\overline{P}_C=\frac{M-1}{M}. \tag{20}$$

Here, $\Pr(M_m^S)=\frac{1}{M},\ \forall m\in\{1,\ 2,\ldots,M\}$ happens only if

$$\Pr(\alpha_{i-j}=0)=\Pr(\alpha_{i-j}=1)=\frac{1}{2},\quad \forall j. \tag{21}$$

Therefore, from (6), we get

$$\begin{aligned}&\Pr(y(j)\le\tau_S(j))=\Pr(y(j)>\tau_S(j))=\frac{1}{2},\quad\forall j.\\&\Rightarrow\tau_S(j)=\tau_S^{opt}(j)=\tau_S^{Median}=\frac{\ln 2}{\lambda_S},\end{aligned} \tag{22}$$

where (22) is given by the median of the exponential distribution y. Hence, the optimal threshold at S, when the channels $S-D$ and $S-E$ are independent is given by the median of y. ■

Remark 1. *In the case of independent channels, it can be noted that with a proper choice of $\tau_S(j)$ at S, SER at E can be made as high as $\frac{M-1}{M}$, which is independent of $\tau_E(j)$ chosen at E.*

B. SER at E-Correlated Channels

When E is located close to D, there is likely to be a correlation between the channels $S-D$ and $S-E$ [20, Chapter. 3]. Therefore, designing thresholds when the channels $S-D$ and $S-E$ are correlated is an interesting case to study. If the channels $S-D$ and $S-E$ are correlated then $x(j)$ and $y(j)$ are exponentially correlated random variables. For notational convenience, $x(j)$ and $y(j)$ are represented as x_j and y_j respectively. The joint probability density function $f(x_j,y_j)$ of the bivariate exponential distribution is given as [21],

$$f\left(x_j,y_j\right)=\frac{\lambda_S\lambda_E}{1-\rho}e^{-\frac{x_j\lambda_E+y_j\lambda_S}{1-\rho}}I_0\left(\frac{2\sqrt{\rho x_j y_j\lambda_E\lambda_S}}{1-\rho}\right), \tag{23}$$

where ρ is the correlation coefficient between x, y and $I_0(.)$ is modified Bessel function of first kind and order zero. Now the SER at E is given as,

$$\overline{P}_E=\int_0^\infty\cdots\int_0^\infty P_E\times f\left(x_j,y_j\right)dx_jdy_j, \tag{24}$$

which is difficult to solve in this form. However, the SER can also be derived from the expectation of P_C. Where, the expectation of P_C in (10), contains the summation of terms of the form,

$$\mathbb{E}\left[t_{|m_1-m_2|}^i\Pr(M_{m_2}^E,M_{m_1}^S)\right]=\mathbb{E}\left[t_{|m_1-m_2|}^i B(m_2)A(m_1)\right]. \tag{25}$$

$A(m_1)$ is the m_1^{th} row of the fourth column in Table I. Each element in the fourth column of Table I are all zeros except for m_1^{th} row. Similarly, $B(m_2)$ is the non-zero element of the column B in the table that can be formed for the eavesdropper. Now, $A(m_1)B(m_2)$ is given as,

$$\begin{aligned}&A(m_1)B(m_2)=\prod_{j=(i+1-\log_2 M)}^{i}g_{m_1}(\alpha_{i-j})g_{m_2}(\beta_{i-j}),\\&g_{(.)}(\alpha_{i-j})\in\left\{\alpha_{i-j},\overline{\alpha}_{i-j}\right\},\quad g_{(.)}(\beta_{i-j})\in\left\{\beta_{i-j},\overline{\beta}_{i-j}\right\}.\end{aligned} \tag{26}$$

here $g_{(.)}(\alpha_{i-j})=g_{(.)}(\beta_{i-j})=1$, for the region specified by the first three columns of the Table I. Since, each channel block is fading independently, and $t_{|m_1-m_2|}^i$ exclusively depends on i^{th} channel block alone, (25) can be written as,

$$\begin{aligned}&\mathbb{E}\left[t_{|m_1-m_2|}^i\prod_{j=(i+1-\log_2 M)}^{i}g_{m_1}(\alpha_{i-j})g_{m_2}(\beta_{i-j})\right]\\&=\mathbb{E}\left[t_{|m_1-m_2|}^i g_{m_1}(\alpha_0)g_{m_2}(\beta_0)\right]\prod_{j\neq i}\mathbb{E}\left[g_{m_1}(\alpha_{i-j})g_{m_2}(\beta_{i-j})\right]\end{aligned} \tag{27}$$

Further, from (26), considering the possible alphabets taken by $g_{m_1}(\alpha_{i-j})$ and $g_{m_2}(\beta_{i-j})$ and using the formulation given in (6), there are four integral forms for $\mathbb{E}\left[g_{m_1}(\alpha_{i-j})g_{m_2}(\beta_{i-j})\right]$, which are given as,

$$\mathbb{E}[\alpha_{i-j}\beta_{i-j}]=\int_0^{\tau_S(j)}\int_0^{\tau_E(j)}f(x_j,y_j)dx_jdy_j, \tag{28a}$$

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/JIOT.2018.2842056, IEEE Internet of Things Journal

$$\mathbb{E}[\overline{\alpha}_{i-j}\beta_{i-j}] = \int_{\tau_S(j)}^{\infty}\int_{0}^{\tau_E(j)} f(x_j,y_j)dx_jdy_j, \quad (28b)$$

$$\mathbb{E}[\overline{\alpha}_{i-j}\overline{\beta}_{i-j}] = \int_{\tau_S(j)}^{\infty}\int_{\tau_E(j)}^{\infty} f(x_j,y_j)dx_jdy_j, \quad (28c)$$

$$\mathbb{E}[\alpha_{i-j}\overline{\beta}_{i-j}] = \int_{0}^{\tau_S(j)}\int_{\tau_E(j)}^{\infty} f(x_j,y_j)dx_jdy_j. \quad (28d)$$

Similarly, $\mathbb{E}\left[t^i_{|m_1-m_2|}g_{m_1}(\alpha_0)g_{m_2}(\beta_0)\right]$ has four integral forms as in (28a-28b) with $t^i_{|m_1-m_2|}$ included in the integral. Although, a closed-form expression for $\mathbb{E}\left[g_{m_1}(\alpha_{i-j})g_{m_2}(\beta_{i-j})\right]$ can be derived, getting a closed-form expression for $\mathbb{E}\left[t^i_{|m_1-m_2|}g(\alpha_0)g(\beta_0)\right]$ is difficult, as it involves the integration of the product of incomplete Gaussian integral $t^i_{(.)}$, exponential functions and Bessel functions. Hence, we try to obtain the thresholds at which E and S operate at their respective optimal performances.

1) Strategy at E to decrease its SER: It is assumed that the knowledge of $\tau_S(j)$ and statistics of $y(j)$ are known at the eavesdropper and will be utilized by E to derive an optimal strategy to decrease its SER.

Lemma 1. *The differential of SER at E ($\overline{P}_E$) w.r.t. $\tau_E(j)$ for each $j \in \{i+1-\log_2 M,\ldots,i\}$ is given by,*

$$\frac{\partial \overline{P}_E}{\partial \tau_E(j)} = C_{i-j} \times G(\tau_E(j),\tau_M(j)),\ C_{i-j} > 0, \quad (29)$$

where,

$$G(\tau_E(j),\tau_S(j)) = 2Q\left(\sqrt{\frac{2\rho\lambda_E\tau_E(j)}{1-\rho}},\sqrt{\frac{2\lambda_S\tau_S(j)}{1-\rho}}\right) - 1, \quad (30)$$

and $Q(.,.)$ is the Marcum Q-function of order one given as [19, eq. (4.11)],

$$Q(v_1,v_2) = \int_{v_2}^{\infty} te^{\frac{-(t^2+v_1^2)}{2}} I_0(v_1t)dt. \quad (31)$$

Proof. See Appendix-A. ∎

Theorem 1. *There exists a unique optimal threshold $\tau_E^{opt}(j)$, given in (32), $\forall j \in \{i,\ (i-1),\ldots,(i+1-\log_2 M)\}$, which leads to the minimum SER at E.*

$$\tau_E^{opt}(j) = \begin{cases} 0 & \tau_S(j) \le \tau_S^{th} \\ \tau_E^*(j) & \tau_S(j) > \tau_S^{th} \end{cases}, \quad (32)$$

where,

$$\tau_S^{th} = \frac{(1-\rho)\ln 2}{\lambda_S},\ \textit{and } \tau_E^* \textit{ is the root of } (30)$$

Proof. [1, Proposition. 2] proves that (29) in Lemma 1 is positive for $\tau_S(j) \le \tau_S^{th}$, and has a unique root $\tau_E^*(j)$ for $\tau_S(j) > \tau_S^{th}$ at which $\overline{P}_E$ is minimized. Hence, the optimal threshold of operation at E is given as $\tau_E^{opt}(j)$. ∎

Corollary 1.1. *$\tau_E^*(j)$ is an increasing function of $\tau_S(j)$.*

Proof. Since, $G(\tau_E(j),\tau_S(j))$ is monotonically increasing and decreasing with $\tau_E(j)$ and $\tau_S(j)$ respectively [22], as we increase $\tau_S(j)$, $G(.,.)$ decreases. Since $\tau_E^*(j)$ is the root of (30), $\tau_E^*(j)$ needs to be increased in order to make $G(.,.) = 0$. Therefore, $\tau_E^*(j)$ is an increasing function of $\tau_S(j)$. ∎

2) Strategy at S to increase SER at E: We assume that E is operating at its optimal threshold and then evaluate the threshold at S for this worst case scenario.

Lemma 2. *The differential of $\overline{P}_E$ w.r.t. $\tau_S(j)$ is given by (62) in Appendix-C, where the differential*

$$\frac{\partial \overline{P}_E}{\partial \tau_S(j)} \ge 0, \quad for\ \tau_S(j) \le \tau_S^{th} \quad (33a)$$

$$= D_{i-j}\left[\int_{\tau_E^*(j)}^{\infty} q(x)f(x,\tau_S(j))dx - \int_{0}^{\tau_E^*(j)} q(x)f(x,\tau_S(j))dx\right],\ D_{i-j} > 0, \tau_S(j) > \tau_S^{th} \quad (33b)$$

where $0 \le q(x) \le 1$.

Proof. See Appendix-C ∎

Theorem 2. *There exists a unique optimal threshold $\tau_S^{opt}(j) \ge \tau_S^{th}$, $\forall j \in \{i+1-\log_2 M,\ldots,\ i\}$ which maximizes the SER at E, operating at its optimal threshold $\tau_E^{opt}(j)$.*

Proof. Using the Corollary 1.1 and Lemma 2, [1, Proposition. 3] proves that there exists a unique optimal threshold $\tau_S^{opt}(j) \ge \tau_S^{th}$ at which $\overline{P}_E$ is maximized. Hence obtaining an optimal threshold of operation at S. ∎

C. Effect of imperfect CSI on destination's performance

Imperfections in CSI estimated at both S and D are due to the presence of noise at their respective receivers. These imperfections in CSI cause a mismatch in the mappings that are selected at S and D, and hence, induces an error at D. Estimated CSI at S and D are respectively given as [23],

$$h_S = h_M + \epsilon_1, \quad h_D = h_M + \epsilon_2, \quad (34)$$

where ϵ_1 and ϵ_2 are complex Gaussian with distribution $\mathcal{CN}(0,\sigma^2)$. Now, h_S and h_M are correlated complex Gaussian random variables with correlation coefficient,

$$\hat{\rho}_{SD} = \frac{Cov\left(h_S,h_D\right)}{\sqrt{Var(h_S)}\sqrt{Var(h_D)}} = \frac{\frac{1}{\lambda_S}}{\frac{1}{\lambda_S}+\sigma^2} = \frac{1}{1+\lambda_S\sigma^2}. \quad (35)$$

Therefore, $|h_S|^2 = y_1$ and $|h_D|^2 = y_2$ are exponentially correlated random variables with correlation coefficient, $\rho_{SD} = |\hat{\rho}_{SD}|^2$, [21, Appendix]. Hence, for a chosen threshold at S, D can optimize its threshold for minimizing its SER following the analysis given in Theorem 1. It should be noted that the correlation in this case will be quite high, as the mismatch in the estimated CSI occurs due to the imperfections at the receivers and not due to the lack of reciprocity (which is the case for the eavesdropper).

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/JIOT.2018.2842056, IEEE Internet of Things Journal

$$P_E^{L_1} = e^{-\lambda_S \tau_S}\left[2Q\left(\sqrt{\frac{2\lambda_E\tau_E}{1-\rho}},\sqrt{\frac{2\rho\lambda_S\tau_S}{1-\rho}}\right)-1\right]+2Q\left(\sqrt{\frac{2\rho\lambda_E\tau_E}{1-\rho}},\sqrt{\frac{2\lambda_S\tau_S}{1-\rho}}\right)\left[\frac{2\lambda_E}{2\lambda_E+c}e^{-\left(\frac{c+2\lambda_E}{2}\right)\tau_E}-e^{-\lambda_E\tau_E}\right]$$
$$+\frac{2\lambda_E}{2\lambda_E+c}\left[e^{-\frac{(c+2\lambda_E)\lambda_S\tau_S}{2\lambda_E+c(1-\rho)}}\left\{-2Q\left(\sqrt{\frac{(2\lambda_E+c(1-\rho))\tau_E}{1-\rho}},\sqrt{\frac{4\rho\lambda_E\lambda_S\tau_S}{(1-\rho)(2\lambda_E+c(1-\rho))}}\right)+1\right\}-e^{-\left(\frac{2\lambda_E+c}{2}\right)\tau_E}\right]+e^{-\lambda_E\tau_E} \quad (36)$$

V. Lower-Bound on SER

Although, finding optimal thresholds at S and D is important, a closed-form expression for SER will be useful for analyzing the system performance. Since the integral in (24) involves an incomplete Gaussian integral $t^i_{(.)}$, exponential and Bessel functions, it is difficult to find a closed-form expression for SER. However, we derive a lower-bound on the SER. Representing $\overline{P}_E$ from (16) as,

$$\begin{aligned}
&= 1-\mathbb{E}\left[t_0^i\right]-\mathbb{E}\left[(t^i_{\frac{M}{2}}-t_0^i)\sum_{m=1}^{M}\Pr(M_m^E M^S_{\frac{M}{2}+m})\right]\\
&-\mathbb{E}\left[(t_1^i-t_0^i)\sum_{m=1}^{M}\left[\Pr(M_m^E M^S_{m+1})+\Pr(M_m^E M^S_{M+m-1})\right]\right]\\
&\ldots-\mathbb{E}\left[(t^i_{\frac{M}{2}-1}-t_0^i)\sum_{m=1}^{M}\Pr(M_m^E M^S_{m+\frac{M}{2}-1})\right] \quad (37)\\
&-\mathbb{E}\left[(t^i_{\frac{M}{2}-1}-t_0^i)\sum_{m=1}^{M}\Pr(M_m^E M^S_{\frac{M}{2}+1+m})\right],
\end{aligned}$$

where a closed-form expression for $1-\mathbb{E}[t_0^i]$ is given by the average SER for conventional M-PSK in Rayleigh fading scenario, [19, eq. (5.68)]. Further, using the formulation in Appendix-E, we derive,

$$\begin{aligned}
t_0^i(x) &\geq 1-\frac{M-1}{M}\times\exp\left(-x\sin^2\left(\frac{\pi}{M}\right)\right),\\
t^i_{\frac{M}{2}}(x) &\leq \frac{1}{M}\times\exp\left(-x\sin^2\left(\frac{M-1}{M}\pi\right)\right), \quad (38)\\
t_k^i(x) &\leq \frac{M-(2k-1)}{2M}\exp\left(-x\sin^2\left(\frac{2k-1}{M}\pi\right)\right), k<\frac{M}{2}
\end{aligned}$$

Using (27), (38) and [22, eqs. (36), (37)], we derive a lower-bound on the SER at E. Due to space limitations, steps to derive the lower-bound and the expression for the bound on SER are omitted. However, we plot the lower-bound on SER for M-PSK in Section VII. For completeness we provide the derived bound for BPSK below and the bounds for M-PSK can be derived similarly. The lower-bound on the SER of BPSK is given as,

$$P_E^L = \frac{1}{2}\left(1-\sqrt{\frac{c}{c+2\lambda_E}}\right)+P_E^{L_1}, \quad (39)$$

and $P_E^{L_1}$ is given by (36) at the top of the page. The first term in (39) is the average BER of conventional BPSK in Rayleigh fading [19, eq. (5.6)].

VI. Discussion on Computational Complexity and Energy Efficiency

In this section, we compare the computational complexity and energy efficiency of the proposed scheme with the benchmark schemes which are used to enhance the security of information transfer. Conventional PLS techniques using artificial noise for multiple input multiple output (MIMO) systems require the generation of null space which incurs a higher complexity. While, the proposed CBMD has to select a mapping which has a non-zero entry of 'A' in Table I, hence, has much lower complexity. Techniques using artificial noise spend ηP, where $0 \leq \eta \leq 1$, power on the information signal, and $(1-\eta)P$ power on the artificial noise. Whereas, CBMD spends the entire power P on the information signal. Hence, CBMD is more energy efficient and low complex. This makes it suitable for IoT platforms. More details on comparison of complexity and energy efficiency of such techniques can be found in [11].

VII. Results

In this section, we assume that the eavesdropper chooses its optimal threshold τ_E^{opt} (Theorem 1), thereby, considering the worst-case scenario for secure information transfer from S to D.

In Fig. 4, variation of the SER for various PSK modulations w.r.t. the received SNR at both E and D is shown. In this figure, considering $\rho = 0.4$, SER at E is plotted for different values of τ_S chosen at S, including the optimal threshold τ_S^{opt} derived in Theorem 2, and a few other heuristic thresholds τ_S^{Median} and τ_S^{th}. It can be clearly seen that for all the modulation orders, SER at D keeps decreasing as the received SNR increases. However, due to the finite error induced by CBMD, SER at E decreases first and then saturates to a high SER. Further, it can be seen that the highest SER is induced for τ_S^{opt}, when compared to the other thresholds, corroborating Theorem 2. It can be observed that τ_S^{Median} performs quite close to τ_S^{opt}, and hence a good option to be chosen as a sub-optimal threshold independent of the channel statistics of E with low complexity. Further, the SER at D when imperfect CSI at both S and D is considered for different modulation orders and are plotted as dashed curves in Fig. 4. For simulation purpose, CSI error with a variance of 1% of the average SNR is considered at both S and D. It can be seen that the performance with the imperfect CSI at D marginally

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/JIOT.2018.2842056, IEEE Internet of Things Journal

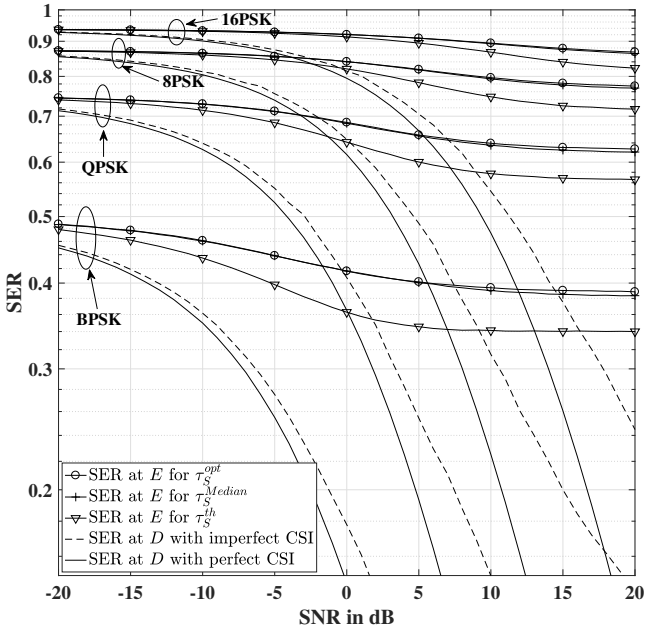


Fig. 4: SER Vs. SNR at E and D for different values of M and τ_S at $\rho = 0.4$.

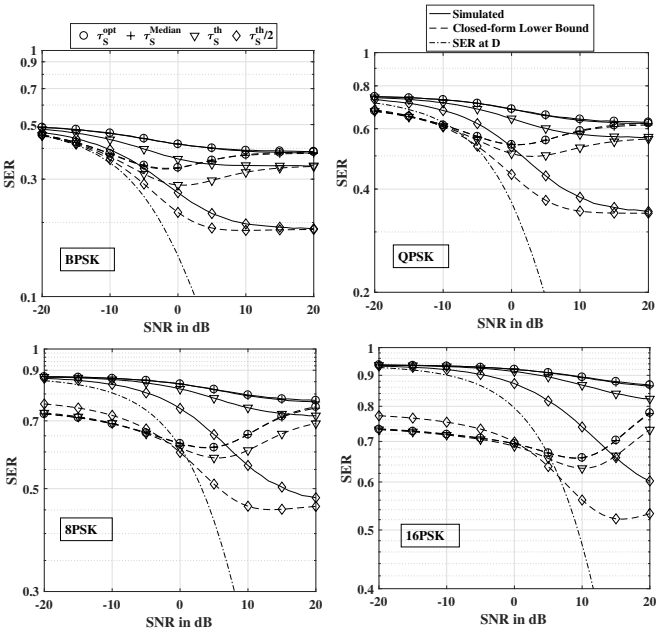


Fig. 6: SER Vs. SNR in dB at a $\rho = 0.4$. Both simulated SER and closed-form lower bounds on SER are plotted for different values of M and τ_S.

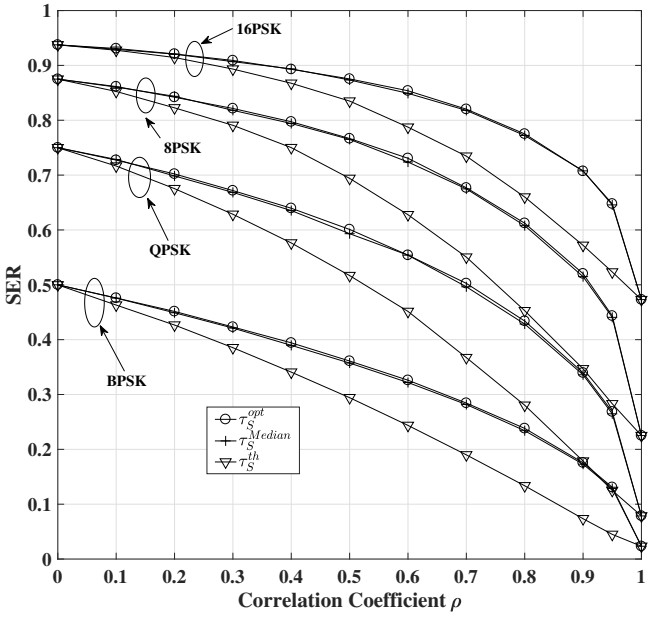


Fig. 5: SER Vs. ρ, for various τ_S, with a 10 dB SNR at E.

deteriorates, therefore we use the optimal threshold at D for minimizing its SER using analysis given given similar to that of Theorem 1.

Fig. 5 shows the variation of SER at E w.r.t. ρ at a received SNR of 10 dB for various chosen thresholds and modulation orders. It can be seen that as ρ increases, SER at E decreases, leading to a reduced level of security. It can also be seen that for all the considered modulation orders, τ_S^{opt} induces the highest SER, which is quite close to τ_S^{Median}. However, for τ_S^{th}, the performance is quite poor compared to other thresholds, and in some cases SER induced by τ_S^{th} is lower than the SER induced by a few lower order modulations operating at τ_S^{opt} and τ_S^{Median}. Therefore, choosing an appropriate threshold for inducing a high SER is very important in this scheme. It can be seen that the effect of ρ is more pronounce on SER at higher levels of ρ. Hence, for practical correlation scenarios, when ρ lies in the range of $[0, 0.5]$ due to the close proximity [20, Chapter. 3], the induced SER stays high, thereby making the job difficult for E in decoding the legitimate data. It is also interesting to see that for $\rho = 0$, SER is $\frac{M-1}{M}, \forall\ M$, and for all the considered thresholds, since $\tau_S = \tau_S^{opt} = \tau_S^{Median} = \tau_S^{th} = \frac{\ln 2}{\lambda_S}$, validating Proposition 1.

In Fig. 6, both the simulated SER and a closed-form lower-bound on the SER are plotted against SNR in dB at $\rho = 0.4$. It can be seen that the bounds are tight at high SNR region for all the modulation orders. It can also be observed that the bounds are tighter for BPSK compared to other modulations at moderate SNR, reason being that the bound derived for t_k^i in (38) is loose in low and moderate SNR regions. One can further tighten the bounds using the bounds derived in [24] with increased complexity. Further, the bounds on SER for the thresholds of interest (τ_S^{opt}, τ_S^{Median}) are tighter than the other less interested thresholds at both moderate and high SNR regions for all the modulation orders.

In Fig. 7, both the simulated SER and a closed-form lower-bound on the SER are plotted against the correlation coefficient ρ at a received SNR of 10 dB at E. It can be seen that the bounds are tighter for lower order modulations, as the tightness of the bound on t_k^i in (38) is a bit loose for higher order modulations. It can further be observed that the tightness increase as the correlation coefficient ρ increases. Further, as seen in Fig. 6, bounds are tighter for the thresholds that are

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/JIOT.2018.2842056, IEEE Internet of Things Journal

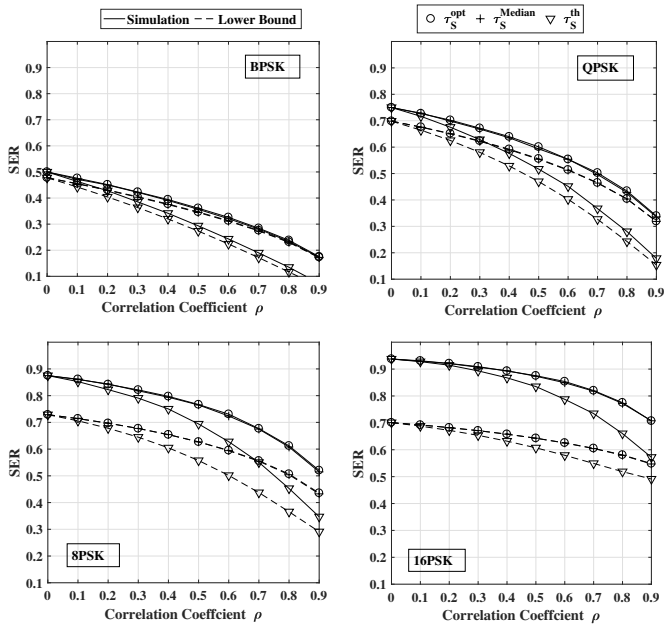


Fig. 7: SER at E Vs. ρ at a received SNR of 10 dB at E. Both simulated SER and closed-form lower bounds on SER are plotted for different values of M and τ_S.

of interest than the other thresholds.

VIII. Conclusion

We proposed CBMD to effectively enhance the security at physical layer of resource-limited IoT devices. It is shown that by properly designing a mapping selection strategy, maximum possible SER can be induced at the eavesdropper, when the legitimate receiver is sufficiently separated from the adversary. Thresholds of operation at the adversary and the legitimate nodes have been derived for their respective optimal performances when the main and adversary's channels are correlated. It is observed from the simulation results that for a practical scenario of correlated channels, the induced SER at the adversary is quite high. Further, a closed-form expression for a lower-bound on the SER at the adversary is derived for CBMD. Looking at future directions, analysis done for the proposed schemes will help in paving a way for designing new techniques in future for securing devices with limited resources, and in situations where the eavesdropper is located close to the destination.

Appendix

A. Proof for Lemma 1

We differentiate $\overline{P}_C$ instead of $\overline{P}_E$ and take a negative of the obtained expression. Since each channel block is independently fading, we differentiate $\overline{P}_C$ w.r.t. $\tau_E(j)$, $\forall j \in \{i = i+1-\log_2 M, \ldots, i\}$ one after the other. Now, considering the differential of terms with t_0^i in (16), for $j = i+1-\log_2 M$, we have,

$$\frac{\partial}{\partial \tau_E(j)} \mathbb{E}\left[t_0^i \sum_{m=1}^{M} \Pr(M_m^E M_m^S) \right]. \tag{40}$$

Using the formulation in Table II and from (27), (40) can be written as,

$$= \sum_{m=1}^{M} \Bigg\{ \underbrace{\frac{\partial \left\{ \mathbb{E}\left[g_m(\alpha_{i-j}) g_m(\beta_{i-j}) \right] \right\}}{\partial \tau_E(j)}}_{d_{i-j,0}^{m,m}} \times \underbrace{\mathbb{E}\left[t_0^i \prod_{\hat{j} \neq j} g_m(\alpha_{i-\hat{j}}) g_m(\beta_{i-\hat{j}}) \right]}_{C_{i-j,0}^{m,m}} \Bigg\}, \tag{41}$$

where the super script of both C and d represent the element's position in Table II and the subscripts $(i-j)$ and t_0^i denote that we are differentiating w.r.t. $\tau_E(j)$ while considering the terms having t_0. Due to the Toeplitz symmetric nature of Table II and Gray coded mapping assignment of it, for t_0^i, each $d_{i-j,0}^{m,m}$ has a conjugate $\overline{d}_{i-j,0}^{m,m}$ with a same coefficient as,

$$C_{i-j,0}^{M+1-m,M+1-m} = C_{i-j,0}^{m,m}. \tag{42}$$

Where the conjugate $\overline{d}_{i-j,0}^{m,m}$ is given as $d_{i-j,0}^{M+1-m,M+1-m}$,

$$\overline{d}_{i-j,0}^{m,m} = \frac{\partial \left\{ \mathbb{E}\left[\overline{g}_m(\alpha_{i-j}) \overline{g}_m(\beta_{i-j}) \right] \right\}}{\partial \tau_E(j)}, \quad \overline{g}_{(.)} = 1 - g_{(.)}. \tag{43}$$

Now, the conjugates having the same coefficient $C_{i-j,0}^{m,m}$, can be added together. Therefore, (41) can be written as,

$$= \sum_{m=1}^{M/2} \left\{ \left[\overline{d}_{i-j,0}^{m,m} + d_{i-j,0}^{m,m} \right] \times C_{i-j,0}^{m,m} \right\}. \tag{44}$$

Here, $C_{(.)}^{(.)}$ is an expectation of a non-negative number, hence positive. Since the merged two terms are conjugates, from the possible alphabets of $g(.)$ given in (26), we have,

$$\overline{d}_{i-j,0}^{m,m} + d_{i-j,0}^{m,m} = \begin{cases} \frac{\partial \mathbb{E}[\alpha_{i-j}\beta_{i-j} + \overline{\alpha}_{i-j}\overline{\beta}_{i-j}]}{\partial \tau_E(j)} \\ \frac{\partial \mathbb{E}[\overline{\alpha}_{i-j}\beta_{i-j} + \alpha_{i-j}\overline{\beta}_{i-j}]}{\partial \tau_E(j)} \end{cases}. \tag{45}$$

In particular, for the terms with t_0^i, it is the first term of (45). Now, using (46) given in the top of next page (derived in Apppendix-D), the differential of $\overline{P}_C$ w.r.t. $\tau_E(j)$ for the terms with t_0^i is given as,

$$= -G\left(\tau_E(j), \tau_S(j)\right) \times \underbrace{\sum_{m=1}^{M/2} C_{i-j,0}^{m,m}}_{C_{i-j,0}} \tag{47}$$

Now, differentiating the terms containing t_k^i, $k \in \{1, \ldots, \frac{M}{2}\}$ w.r.t. $\tau_E(j)$, for $j = i+1-\log_2 M$. We use Table II and (27)

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/JIOT.2018.2842056, IEEE Internet of Things Journal

$$\frac{\partial}{\partial\tau_E(i)}\mathbb{E}\left[t_k^i\left(\alpha_0\overline{\beta}_0+\overline{\alpha}_0\beta_0\right)\right]=-\frac{\partial}{\partial\tau_E(i)}\mathbb{E}\left[t_k^i\left(\alpha_0\beta_0+\overline{\alpha}_0\overline{\beta}_0\right)\right]=t_k^i(\tau_E(i))G\left(\tau_E(i),\tau_S(i)\right) \tag{46}$$

For steps see Appendix − D

to get,

$$\frac{\partial}{\partial\tau_E(j)}\mathbb{E}\left[t_k^i\sum_{m=1}^{M}\left\{\Pr(M_m^EM_{m+k}^S)+\Pr(M_m^EM_{m+M-k}^S)\right\}\right]$$
$$=\sum_{m=1}^{M}\Bigg\{\underbrace{\frac{\partial}{\partial\tau_E(j)}\mathbb{E}\left[g_m(\alpha_{i-j})g_{m+k}(\beta_{i-j})\right]}_{d_{i-j,k}^{m,m+k}}\times C_{i-j,k}^{m,m+k}+$$
$$\underbrace{\frac{\partial}{\partial\tau_E(j)}\mathbb{E}\left[g_m(\alpha_{i-j})g_{M+m-k}(\beta_{i-j})\right]}_{d_{i-j,k}^{m,M+m-k}}\times C_{i-j,k}^{m,M+m-k}\Bigg\}, \tag{48}$$

where

$$C_{i-j,k}^{m,m+k}=\prod_{\hat{j}\neq j}\mathbb{E}\left[t_k^ig_m(\alpha_{i-\hat{j}})g_{m+k}(\beta_{i-\hat{j}})\right],$$
$$C_{i-j,k}^{m,M+m-k}=\prod_{\hat{j}\neq j}\mathbb{E}\left[t_k^ig_m(\alpha_{i-\hat{j}})g_{M+m-k}(\beta_{i-\hat{j}})\right]. \tag{49}$$

Again, due to the Toeplitz symmetric nature of Table II and the Gray coded mapping assignment, conjugates with same coefficients are available for both $d_{i-j,k}^{m,m+k}$ and $d_{i-j,k}^{m,M+m-k}$. It can be seen that the conjugates having the same coefficients are,

$$C_{i-j,k}^{M+1-m,M+1+k-m}=C_{i-j,k}^{m,m+M-k},$$
$$C_{i-j,k}^{M+1-m,M+1-k-m}=C_{i-j,k}^{m,m+k}. \tag{50}$$

Therefore, (48) can be written as,

$$\sum_{m=1}^{M}\frac{\partial}{\partial\tau_E(j)}\left[d_{i-j,k}^{m,m+k}+\overline{d}_{i-j,k}^{m,m+k}\right]\times C_{i-j,k}^{m,m+k}, \tag{51}$$

which can further be simplified using (45) and (46) given in the top of next page (derived in Apppendix-D) as,

$$=-G\left(\tau_E(j),\tau_S(j)\right)\times\underbrace{\sum_{m=1}^{M}\pm\,C_{i-j,k}^{m,m+k}}_{C_{i-j,k}} \tag{52}$$

Therefore, adding all the differentials w.r.t. $\tau_E(j)$ of all k, for $j=i+1-\log_2 M$, we get,

$$\frac{\partial\overline{P}_C}{\partial\tau_E(j)}=-G(\tau_E(j),\tau_M(j))\times C_{i-j}, \tag{53}$$

where $C_{i-j}=\sum_k C_{i-j,k}>0$, shown in Appendix-B. Now for other j, Topelitz symmetric nature and Gray coding assignment ensures the existence of conjugates having same coefficients,

$$C_{i-j,k}^{M+1-m+2^{i-j},M+1-k-m+2^{i-j}}=C_{i-j,k}^{m+2^{i-j},m+k+2^{i-j}},$$
$$C_{i-j,k}^{M+1-m+2^{i-j},M+1+k-m+2^{i-j}}=C_{i-j,k}^{m+2^{i-j},m-k+2^{i-j}}. \tag{54}$$

Hence, following similar steps as in for $j=i+1-\log_2 M$, we get,

$$\frac{\partial\overline{P}_C}{\partial\tau_E(j)}=-G(\tau_E(j),\tau_M(j))\times C_{i-j},\ \forall j. \tag{55}$$

B. Proof for $C_{i-j}>0$

We again use the Toeplitz symmetric nature and Gray coded mapping assignment of Table II along with the properties of t_k^i to show that $C_{i-j}>0$. Proof is provided for $j=i+1-\log_2 M$ and the proof for other j follows similarly.

From (46) given in the top of the page (derived in Apppendix-D), each coefficient of $C_{i-j,k}^{m,m+k}$ in (51) takes either $G(.,.)$ or $-G(.,.)$. Further, from Table II, it can be seen that $C_{i-j,k}^{m,m+k}$ and $C_{i-j,M-k-1}^{m,M+1-(m+k)}$ have same regions of expectations i.e.,

$$\prod_{\hat{j}\neq j}g_m(\alpha_{i-\hat{j}})g_{m+k}(\beta_{i-\hat{j}})=\prod_{\hat{j}\neq j}g_m(\alpha_{i-\hat{j}})g_{M-m-k+1}(\beta_{i-\hat{j}}), \tag{56}$$

These expectations have t_k^i and t_{M-k+1}^i respectively inside them. Essentially, we consider the $C_{(.)}^{(.)}$ with the same regions of expectations of a row in Table II. Therefore, the considered $C_{(.)}^{(.)}$s of same row have the coefficients in (51) as,

$$\frac{\partial}{\partial\tau_E(j)}\mathbb{E}\left[d_{i-j}^{m,m+k}+\overline{d}_{i-j}^{m,m+k}\right] \tag{57}$$
$$=-G(\tau_E(j),\tau_S(j)),\ \left(\frac{M}{2}-m\right)\left(\frac{M}{2}-(m+k)\right)>0,$$
$$\frac{\partial}{\partial\tau_E(j)}\mathbb{E}\left[d_{i-j}^{m,M-m-k}+\overline{d}_{i-j}^{m,M-m-k}\right] \tag{58}$$
$$=G(\tau_E(j),\tau_S(j)),\ \left(\frac{M}{2}-m\right)\left(\frac{M}{2}-(m+k)\right)<0.$$

Further, we have from the Gaussian integral given in Appendix-E,

$$t_k^i-t_{M-(k+1)}^i>0,\ for\ k\in\left\{0,\ 1,\ldots,\frac{M}{2}\right\} \tag{59}$$

Therefore, taking $G(.,.)$ as a common factor in (52), 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/JIOT.2018.2842056, IEEE Internet of Things Journal

updated coefficient of $G(.,.)$ is given as,

$$C_{i-j}^{m,m+k} = \prod_{\hat{j}\neq j} \mathbb{E}\left[t_k^i g_m(\alpha_{i-\hat{j}}) g_{m+k}(\beta_{i-\hat{j}})\right] - \prod_{\hat{j}\neq j} \mathbb{E}\left[t_{M-(k+1)}^i g_{M-m+1}(\alpha_{i-\hat{j}}) g_{M-(m+k)+1}(\beta_{i-\hat{j}})\right] > 0. \quad (60)$$

Hence, adding all the terms leads to a positive coefficient,

$$C_{i-j} = \sum_m \sum_k C_{i-j}^{m,m+k} > 0. \quad (61)$$

C. Proof for Lemma 2

We differentiate $\overline{P}_E$ w.r.t. $\tau_S(j)$, $\forall j \in \{i+1-\log_2 M, \ldots, i\}$, assuming that E uses its optimal threshold. Again using the Leibniz rule and following a similar analysis to that of Appendix-A, ignoring the arguments of τ_S and τ_E^{opt}, we get,

$$\frac{\partial \overline{P}_E}{\partial \tau_S}|_{\tau_E^{opt}} = D_{i-j} \times \left\{ \frac{\partial \tau_E^{opt}}{\partial \tau_S} \times \int_0^{\tau_S} q(\tau_E^{opt}) f(\tau_E^{opt}, y) dy - \frac{\partial \tau_E^{opt}}{\partial \tau_S} \times \int_{\tau_S}^{\infty} q(\tau_E^{opt}) f(\tau_E^{opt}, y) dy + \int_{\tau_E^{opt}}^{\infty} q(x) f(x, \tau_S) dx - \int_0^{\tau_E^{opt}} q(x) f(x, \tau_S) dx \right\}, \quad (62)$$

where $D_{i-j} \geq 0$. Since $q(x)$ depends only on $x(i)$, $q(x(j)) = 1$ for $j \neq i$ and for $j = i$, $0 \leq q(x) < 1$. For $\tau_S \in [0, \tau_S^{th}]$, from Theorem 1, $\tau_E^{opt} = 0$, implying (62) is always positive for $\tau_S \leq \tau_S^{th}$. Now for $\tau_S > \tau_S^{th}$, we have,

$$\frac{\partial \overline{P}_E}{\partial \tau_S}|_{\tau_E^{opt}} = D_{i-j} \left\{ -\lambda_E e^{-\lambda_E \tau_E^*} q(\tau_E^*) \frac{\partial \tau_E^*}{\partial \tau_S} G(\tau_E^*, \tau_S) \int_{\tau_E^*}^{\infty} q(x) f(x, \tau_S) dx - \int_0^{\tau_E^*} q(x) f(x, \tau_S) dx \right\}. \quad (63)$$

Since, τ_E^* is a solution of $G(., \tau_S) = 0$, we get (33b).

D. Steps for deriving (46)

Without loss of generality, ignoring the arguments, superscripts and subscripts, we add the differentials of (28a) and (28c) to get,

$$\frac{\partial \mathbb{E}\left[\alpha\beta + \overline{\alpha}\overline{\beta}\right]}{\partial \tau_E} = \frac{\partial}{\partial \tau_E} \left\{ \int_0^{\tau_S} \int_0^{\tau_E} t_k(x) f(x, y) dx dy + \int_{\tau_S}^{\infty} \int_{\tau_E}^{\infty} t_k(x) f(x, y) dx dy \right\}. \quad (64)$$

Using the Leibniz rule of differential under integration we get,

$$= \int_0^{\tau_S} t_k(\tau_E) f(\tau_E, y) dy - \int_{\tau_S}^{\infty} t_k(\tau_E) f(\tau_E, y) dy \quad (65)$$

Now from (23), (31), the above differential can be simplified as,

$$= t_k(\tau_E) \underbrace{\left[1 - 2Q\left(\sqrt{\frac{2\rho\lambda_E\tau_E}{1-\rho}}, \sqrt{\frac{2\lambda_S\tau_S}{1-\rho}}\right)\right]}_{-G(\tau_E, \tau_S)}. \quad (66)$$

Similarly adding the differentials of (28b) and (28d), we get,

$$\frac{\partial \mathbb{E}\left[\alpha\overline{\beta} + \overline{\alpha}\beta\right]}{\partial \tau_E} = \frac{\partial}{\partial \tau_E} \left\{ \int_0^{\tau_S} \int_{\tau_E}^{\infty} t_k(x) f(x, y) dx dy + \int_{\tau_S}^{\infty} \int_0^{\tau_E} t_k(x) f(x, y) dx dy \right\}.$$

$$= \int_{\tau_E}^{\infty} t_k(\tau_E) f(\tau_E, y) dy - \int_0^{\tau_S} t_k(\tau_E) f(\tau_E, y) dy$$

$$= t_k(\tau_E) \underbrace{\left[2Q\left(\sqrt{\frac{2\rho\lambda_E\tau_E}{1-\rho}}, \sqrt{\frac{2\lambda_S\tau_S}{1-\rho}}\right) - 1\right]}_{G(\tau_E, \tau_S)}. \quad (67)$$

E. Finite integral form of $t_k(x)$

Using the classical formulation given in [25], we derive,

$$t_0^i(x) = 1 - \frac{1}{\pi} \int_0^{\frac{M-1}{M}\pi} \exp\left(-\frac{x \sin^2\left(\frac{\pi}{M}\right)}{\sin^2(\theta + \frac{\pi}{M})}\right) d\theta, \quad (68)$$

$$t_{\frac{M}{2}}^i(x) = \frac{1}{\pi} \int_0^{\frac{\pi}{M}} \exp\left(-\frac{x \sin^2\left(\frac{M-1}{M}\pi\right)}{\sin^2(\theta + \frac{M-1}{M}\pi)}\right) d\theta, \quad (69)$$

$$t_k^i(x) = \frac{1}{2\pi} \left[\int_0^{\frac{M-(2k-1)}{M}\pi} \exp\left(-\frac{x \sin^2\left(\frac{2k-1}{M}\pi\right)}{\sin^2(\theta + \frac{2k-1}{M}\pi)}\right) d\theta - \int_0^{\frac{M-(2k+1)}{M}\pi} \exp\left(-\frac{x \sin^2 \frac{2k+1}{M}\pi}{\sin^2(\theta + \frac{2k+1}{M}\pi)}\right) d\theta \right]. \quad (70)$$

REFERENCES

[1] S. V. Pechetti, A. Jindal, and R. Bose, "Channel-Based mapping diversity for enhancing the physical layer security in the internet of things," in *IEEE PIMRC 2017 Special Session SP-04*, Montreal, Canada, Oct. 2017.

[2] R. Bose, S. V. Pechetti, and A. Jindal, "Physical layer security in a wireless communication channel," Indian Patent Request 201 711 026 638, Jul. 26, 2017.

[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5g wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, April 2015.

[4] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[5] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[9] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *JCM*, vol. 2, pp. 24–32, 2007.

[10] L. Hu, H. Wen, B. Wu, F. Pan, R. F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in internet of things," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2017.

[11] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct 2015.

[12] M. I. Husain, S. Mahant, and R. Sridhar, "Cd-phy: Physical layer security in wireless networks through constellation diversity," in *IEEE MILCOM*, Oct 2012, pp. 1–9.

[13] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1478–1493, Dec 2016.

[14] W. Xiang, S. L. Goff, M. Johnston, and K. Cumanan, "Signal mapping for bit-interleaved coded modulation schemes to achieve secure communications," *IEEE Wireless Communications Letters*, vol. 4, no. 3, pp. 249–252, June 2015.

[15] H. Li, X. Wang, and J. Y. Chouinard, "Eavesdropping-resilient ofdm system using sorted subcarrier interleaving," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1155–1165, Feb 2015.

[16] J. Xu, L. Duan, and R. Zhang, "Transmit optimization for symbol-level spoofing," *IEEE Transactions on Wireless Communications*, vol. 17, no. 1, pp. 41–55, Jan 2018.

[17] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 619–625, April 2013.

[18] ——, "Channel aware encryption and decision fusion for wireless sensor networks," in *2011 IEEE International Workshop on Information Forensics and Security*, Nov 2011, pp. 1–6.

[19] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels: A Unified Approach to Performance Analysis*, 1st ed. New York: Wiley, 2000.

[20] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.

[21] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high snr," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, April 2011.

[22] A. H. Nuttall, "Some integrals involving the q-function," *Naval Underwater Systems Center, New London Lab., New London, Conn.*, vol. Tech. Rep. 4297, Apr 1972.

[23] J. K. Cavers, "An analysis of pilot symbol assisted modulation for rayleigh fading channels [mobile radio]," *IEEE Transactions on Vehicular Technology*, vol. 40, no. 4, pp. 686–693, Nov 1991.

[24] S. H. Chang, P. C. Cosman, and L. B. Milstein, "Chernoff-type bounds for the gaussian error function," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 2939–2944, November 2011.

[25] J. W. Craig, "A new, simple and exact result for calculating the probability of error for two-dimensional signal constellations," in *MILCOM 91 - Conference record*, Nov 1991, pp. 571–575 vol.2.

Sasi Vinay Pechetti (S'17) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT) Bhubaneswar, Bhubaneswar, India, in 2015. He is currently pursuing the Ph.D. degree in electrical engineering from the Indian Institute of Technology (IIT) Delhi, Delhi, India. He was a visiting research assistant in Department of Intelligent Information Engineering and Sciences, Doshisha University, Japan during May-July 2014. His current research interests include, physical layer security, MIMO and HetNets.

Abhishek Jindal (S'08, M'17) received the B.Tech and M.Tech degrees in electronics and communications engineering from the Jaypee Institute of Information Technology (JIIT), Noida, India in 2009 and 2011 respectively. He received the Ph.D. degree from the Bharti School of Telecomm. Tech. and Mgmt. at the Indian Institute of Technology Delhi (IITD), Delhi, India in 2017. He was a post doctoral research associate in the department of computer science at the University of Texas at Dallas (UTD), Dallas, USA during 2017-2018. His research interests include performance study and resource allocation for physical layer security.

Ranjan Bose (M'10 SM'11) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT) Kanpur, Kanpur, India, in 1992 and the M.S. and Ph.D. degrees in electrical engineering from the University of Pennsylvania, Philadelphia, PA, USA, in 1993 and 1995, respectively. From 1996 to 1997, he was with Alliance Semiconductor Inc., San Jose, CA, USA, as a Senior Design Engineer. Since November 1997, he has been with the Department of Electrical Engineering, IIT Delhi, New Delhi, India, where he is currently the Microsoft Chair Professor. His current research interests include broadband wireless access, wireless security, and coding theory.