Engineering Science and Military Technologies
Volume (1) - Issue (2) - Oct 2017

ISSN: 2357- 0954
DOI: 10.21608/ejmtc.2017.1438.1055

Spatial Signature Modulation: A Novel Secure Modulation Approach for MIMO Wiretap Channel

Original Article

Amr Abdelaziz[1], Ashraf D. Elbayoumy[2]

[1]Department of Electrical and Computer Engineering, The Ohio State University, Columbus, Ohio 43201,
[2]Department of Electrical Engineering, Military Technical College, Cairo, Egypt.

Key words:

Angle of arrival, angle of departure, application layer security, joint security, MIMO security, physical layer security, secret key agreement, spatial signature modulation.

Corresponding Author:

Amr M. Abdel-Aziz, Department of Electrical and Computer Engineering, The Ohio State University, Columbus, Ohio, 43210

Abstract

Security in physical and application layers have been always thought of as a complementary paradigm. In this paper, we argue that potential cooperation between physical and application layers provides several advantages and unique features that are not available in each paradigm by itself. The problem of exchanging confidential messages between nodes, A and B, in the presence of an active adversary, E, over an insecure MIMO channel is considered. We introduce a double layer spatial signature modulation (SSM) in which the transmitted information is conveyed into the spatial signature of the transmitting antenna array observed by the intended receiver. Meanwhile, any other eavesdropper does not share the same bearing angle of the legitimate receiver obtains infinitesimally small amount of information. Further, to establish a secure link, A and B are required to share a secret common information prior to communication while keeping E ignorant about it. To that end, we introduce a novel physical layer assisted secret key agreement (SKA) protocol that leverages the cooperation between physical and application layer security. Angle of Arrival (AoA) and Angle of Departure (AoD) are physical layer parameters that can be exploited not only for their well performance at low SNR, but also for their contextual meaning that provides security advantages. In the proposed SKA protocol, AoA is explored as a physical mean for message source authentication, meanwhile, AoD is used as a common source of randomness in a smart signal processing approach to generate secret key bits without any extra communication overhead. We show that E can be kept ignorant about the generated key bit stream conditioned on its physical location. This work introduces the notion of physical hardness to an adversary pursuing either active or passive strategy. After establishing a secret common information, we show that the continuous use of AoA as a mean for message source authenticity provides a considerable advantage against active adversary during the message exchange phase. Extending the proposed scheme to a mobile communication environment is also provided. Finally, quantitative analysis for the security gain due to the potential cooperation between physical and application layer security is developed..

I. INTRODUCTION

Security issues of wireless communication networks is of a great importance due to the vulnerability caused by the untethered nature of the open wireless medium. The use of physical layer properties for message confidentiality has attracted a lot of researchers since the evolution of the definition of the wiretap channel introduced by Wyner[1, 2] and the consequent work of Maurer[3, 4]. However, the proof of existence of secrecy capacity achieving codes was based on nonconstructive random coding arguments. Therefore, extensive researches have been made aiming to define secrecy capacity and achieving code construction, see for example[5, 6, 7]. On the other hand, MIMO technology is embraced as one of the key technologies for fulfilling the drastic increase in throughput demands of future communication systems. In addition to signal diversity and/or spatial multiplexing capabilities offered by MIMO, it inherits many other features that contribute to communication security. The secrecy capacity of MIMO wiretap channel was derived in[8, 9, 10].

A key consideration in the MIMO wiretap channel is the amount of information available about the eavesdropper. In principle, to be able to determine the secrecy capacity of MIMO wiretap channel, either full eavesdropper's

channel state information (CSI) or its distribution is required. When no information is available about the eavesdropper, the secrecy rate optimization problem is ill-posed, and hence secrecy capacity can not be determined. Other security metric are used therefore to assess security performance; e.g. secrecy outage performance for MISO wiretap channel with partial side information was evaluated in[11], whereas it was considered in[12] for the MIMO wiretap channels with multiple jamming signals.

In practical scenarios, this information is very hard to acquire especially when dealing with strictly passive eavesdroppers. In this work, we opt ourselves to more practical scenario where there is only a limited evident information about the possible eavesdropper. In particular, we consider the scenario in which the eavesdropper has a limited access to geographic area of the communication environment, i.e. it may exist, if any, only in a subarea of the communication field. This assumption is well adopted with many real world communication scenarios. For example in naval tactical communications, eavesdroppers are unlikely to lie within the troops.

Based on the knowledge level available about the eavesdropper, several approaches have been considered in the context of MIMO wiretap channel aiming to come up with secrecy capacity, if characterized, achieving scheme or, at least, to minimize the secrecy outage probability. The use of artificial noise (AN)[13], which was adapted to a more practical settings with M-QAM alphabet in[14], is considered even for the case where eavesdropper CSI is available. Assuming more transmitter antenna elements than those at the intended recipient in[15], the AN scheme was redesigned as a one-time pad secret key aligned within the null space of the transmitter to legitimate receiver channel. The results therein assumed only statistical information about eavesdropper channel. When no CSI information about the eavesdropper, transmit antenna selection (TAS) was proposed to enhance physical layer security in MIMO wiretap channels[16, 17]. While, with perfect CSI about both intended receiver and eavesdropper, beamforming toward the intended receiver is shown to be optimal in[18].

Apart from the aforementioned approaches, another line of research concerning the situation where no eavesdropper CSI available is the directional modulation (DM) which was firstly introduced in [19]. The term DM refers to the use of the antenna beam pattern to create the transmitted signal magnitude and phase only in the direction of the intended receiver. Different from conventional beamforming which is designed to provide directional power scaling independent to the transmitted signal, DM use the transmitted signal itself together with the channel matrix to the intended receiver to generate the beamformer. The beamformer is then transmitted through the channel, consequently, the original transmitter signal is reconstructed only at the intended receiver. Several advances are made in the design of DM for enhanced security in MIMO wiretap channel, see for example[20, 21].

In its general form, coding for the wiretap channel uses a double layer sequence of wiretap codes, inner and outer codes. The inner layer ensures that the transmitted message can be reliably decoded by the legitimate receiver, and the outer layer guarantees that the message is kept secret from the eavesdropper. Following the same convention, in this work, contrary to the state of the art directional modulation schemes, we introduce a double layer spatial signature modulation (SSM). Similar to the DM, SSM convey the information into the spatial signature of the transmitting antenna observed by the intended receiver whereas any other eavesdropper does not share the same bearing angle of the legitimate receiver obtains infinitesimally small amount of information. Meanwhile, the major difference between SSM and DM lies in the former dual layer construction. The inner layer ensure that the transmitter spatial signature can be demodulated reliably at the legitimate receiver. Whereas, the outer layer is designed from multiple random spatial signature in order to assure confusion at the eavesdropper.

Building upon the introduced SSM, we introduce a novel joint physical-application layer security scheme that leverages the cooperation between smart signal processing techniques at the physical layer and computational security algorithms at the upper layers.We show that SK reconciliation from physical layer parameters can be established through the physical layer representation of the message exchange of the upper security layers. Thus, extracted SK bits come without any extra communication overhead. We also show that, the joint work between physical layer and upper security layers provides considerable security advantage gained from the contextual meaning of physical layer parameters about the communication channel. The cooperation between physical and upper security layers introduces the notion of physical hardness to the attacker in top of the conventional computational hardness.

A. Related Work

The concept of DM was firstly introduced in[19]. Secure multiple-users transmission using Multi-Path DM was introduced in[22], where the dispersive nature of the wireless channel is exploited to create a position-based secure communication link. Whereas in[23], an orthogonal vector approach is proposed for the synthesis of multi-beam DM transmitters. It was shown that this system has the capability of concurrently projecting independent data streams into different specified spatial directions, while simultaneously distorting signal constellations in all other directions. The authors also used SER simulation to show the advantage of the proposed approach. Meanwhile, the work in[24] proposed an iterative pattern synthesis approach for DM transmitter. This work was the first to offer discussion on constraining DM transmitter far-field radiation patterns so that energy is primarily concentrated in the spatial direction where low SER is to be achieved, while interference projected along other directions is reduced. Recently in[25], the concept of DM via symbol level precoding is employed to enhance the security of

multi-user MIMO wiretap channel with no eavesdropper CSI being available. Meanwhile, perfect CSI of the intended receiver is used to design the symbol level precoder while keeping the eavesdropper in a worse situation, eventhough it has perfect knowledge of main channel CSI. Precoder design was obtained by the solution of linearly constrained quadratic optimization problem using iterative algorithm and non-negative least squares. Also, necessary condition for the existence of optimal precoder for the proposed DM was derived. However, the effect of imperfect main channel CSI has not been addressed. Also, secrecy outage performance was not evaluated, rather, authors used different MIMO receiver structure to assess the ability of a possible eavesdropper to reliably demodulate the signal in terms of symbol error rate (SER).

The concept of using a common source of randomness between two communicating nodes to agree on a common secret information has been extensively studied in literature. In[26], Maurer showed that any public key based SKA can be computationally secured rather it can not be unconditionally secured. Facing an active adversary with unlimited computational power, the proposed an information theoretic SKA from public discussion constitutes observing a sequence of realizations of correlated random variables over an insecure channel.

Later on Maurer's work, much attention has been paid to the exploitation of different common sources of randomness. By exploring its reciprocity, communication channel, which incorporates different parameters, has been exploited for secret key generation. A scheme for SKA based on received signal strength variation has been proposed in[27]. Moreover, SKA based on wireless fading channels based on channel gains quantization with guardband was introduced in[28].

In a relatively recent work[29], Onur *et. al.* introduced a source model SKA that exploits the distance as well as angle between legitimate nodes as the observed common randomness. A substantial information theoretic security analysis was provided with an upper and lower bounds on the maximum achievable secret key rate. While the angle between nodes is considered as a source of common randomness, it has not been used as an authentication tool.

In[30] and the subsequent work[31], secret key agreement protocol based on AoA estimation as a common source of randomness were proposed. The authors developed SKA protocol that can exploit either the Azimuth AoA to generate the secret key or both the Azimuth and Elevation angles to generate the secret key. While, it is true that AoA estimation performs well in low SNR which makes it a good candidate for SKA, the amount of information that an eavesdropper can learn about it was not considered. Assuming that the location of the legitimate nodes is known to the attacker, thus the attacker may know to a certain precision what AoA is expected at the receiver. In other words, attacker equivocation about the secret key has not been studied.

In all of these works, security analysis was developed based on information theoretic arguments that does not assume an adversary with limited computation power. However, none of these works provides a comprehensive solution that covers both SKA phase as well as the confidential message exchange phase.

B. Paper Contributions

We introduce a novel joint physical-application layer security scheme that leverage the cooperation between smart signal processing techniques at the physical layer and computational security algorithms at the upper layers.

We show that SK reconciliation from physical layer parameters can be established through the physical layer representation of the message exchange of the upper security layers. Thus, extracted SK bits comes without any extra communication overhead.

We show that the joint work between physical layer and upper security layers provides considerable security advantage gained from the contextual meaning of physical layer parameters about the communication channel.

The cooperation between physical and upper security layers introduces the notion of physical hardness to the attacker in top of the conventional computational hardness.

We show that the proposed SKA agreement achieves full equivocation for an eavesdropper conditioned on its physical location.

II- SYSTEM MODEL

In the rest of this paper, we use boldface uppercase letters for random vectors/matrices, uppercase letters for their realizations, bold face lowercase letters for deterministic vectors and lowercase letters for its elements. While, (.)* denotes conjugate of complex number, (.)† denotes conjugate transpose, I_N denotes identity matrix of size N, tr(.) denotes matrix trace operator, var(.) denotes variance of random variable, det(.) denotes matrix determinant operator and $1_{m\,x\,n}$ denotes a $_{m\,x\,n}$ matrix of all 1's.

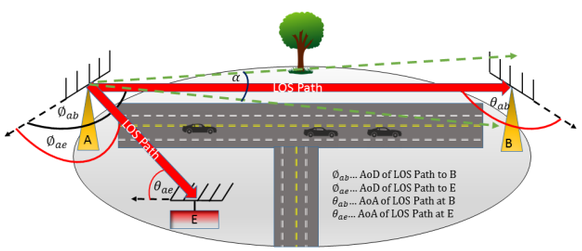

Fig. 1: System Model

A- System model

As illustrated in Fig. (1), we consider the MIMO wiretap channel scenario in which a transmitter A with $N_t > 1$ antennas amounts to transmit a confidential message massage to a receiver, B, having $N_r > 1$ antennas over an insecure channel in the presence of an active adversary, E, equipped with $N_e > 1$ antennas. Nodes A and B are not assumed to share any secret information a prior. We will assume the uniform linear array (ULA) antenna configuration, however, the obtained results apply directly to any other antenna configuration with straightforward

manipulation. Further, we assume a narrowband system under flat fading with a single significant channel tap. The discrete baseband equivalent channel for the signal received by each of the legitimate destination, Y, and the adversary, Z, as follows:

$$\mathbf{Y} = \mathbf{H}_b\mathbf{X} + \mathbf{N}_b, \qquad \text{Eq. 1}$$

$$\mathbf{Z} = \mathbf{H}_e\mathbf{X} + \mathbf{N}_e,$$

where $X \in \mathbb{C}^{Nt \times 1}$ is the transmitted signal vector constrained by an average power constraint $E[tr(XX^{\dagger})] \leq P$. Also, $H_b \in \mathbb{C}^{Nr \times Nt}$ and $H_e \in C^{Ne \times Nt}$ are the channel coefficients matrices between message source, destination and adversary, respectively. Finally, $N_b \in \mathbb{C}^{Nb \times 1}$ and $N_e \in \mathbb{C}^{Ne \times 1}$ are an independent zero mean circular symmetric complex random vectors for both destination and adversary channels, respectively, where $N_b \sim CN(0, R_b)$ where $R_b = \sigma_b^2 I_{Nb}$ and $N_e \sim CN(0, R_e)$ where $R_e = \sigma_e^2 I_{Ne}$. In the rest of this paper, we assume that:
1- Channel realization of H_b is available only at B.
2- A knows only the bearing angle of B and know nothing about E's channel or location.
3- E knows channel realizations for both H_e and H_e, thus, it implicitly knows the bearing angle of B with respect to A.
4- In contrast to[15], we do not assume any particular constraints on the array sizes at A, B or E.

B- Channel Model

Wireless MIMO channel with dominant LOS component is best described by the Rician fading model. In Rician fading model, the received signal can be decomposed into two components; one is the specular component originated from the LOS path and the other is the diffuse component due to ground reflections and scatters from neighboring vehicles and other objects in the environment, or generally the non-line of sight component (NLOS). The LOS component can be considered fixed while the NLOS component can be best described as a Rayleigh fading channel.

$$\mathbf{H} = \mathbf{H}^{los} + \mathbf{H}^{nlos}, \qquad \text{Eq. 2}$$

where H_{los} and H_{nlos} represents the LOS and NLOS components, respectively and

$$\mathbf{H}^{los} = \sqrt{\frac{k}{1+k}}\left(\frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}}\right)\mathbf{\Psi}$$

$$\mathbf{H}^{nlos} = \sqrt{\frac{1}{2(1+k)}}\hat{\mathbf{H}}, \qquad \text{Eq. 3}$$

where k is the Ricean factor that facilitates the contribution of the LOS component to the received signal, $\Psi = a(\theta)a^{\dagger}(\phi)$, $a(\theta)$ and $a(\phi)$ are the antenna array spatial signature (steering vectors) at receiver and transmitter, respectively, θ and ϕ are the AoA and AoD of the transmitted signal, respectively, as shown in Fig. (1). Note that, AoD, ϕ, represents the bearing angle of the receiver with respect to the transmitter antenna array, we assume it to be the only information available at A about B. Meanwhile, $\hat{H} \sim CN(0, I)$ represents the channel coefficients matrix for the NLOS signal component. For the ULA configuration, the entries of the steering vectors are given by **Eq. 4**

$$\mathbf{a}(\theta) = \begin{bmatrix} 1 & z & z^2 & \dots & z^{n-1} \end{bmatrix}^T$$

$$z = e^{-j2\pi\frac{d\sin(\theta)}{\lambda}},$$

where λ d and n are the wavelength of the center frequency of the transmitted signal, array elements spacing and size, respectively. We parametrize the contribution of the NLOS and LOS components to the signal with $\sigma = \sqrt{1/2(1+k)}$, $\mu = \sqrt{k/(1+k)}$, respectively and choose $\mu^2 + 2\sigma^2 = 1$ for simplicity. It worth mentioning that, AWGN and Rayleigh fading channels are in fact limiting cases of the Rician fading channel.

C- Eavesdropper Channel Constraint

In this section, we introduce our assumption about the eavesdropper channel. We introduce a different definition of channel degradation termed Location Degradation. By location degradation we mean the situation in which the eavesdropper is located away from the receiver location in the sense that **Eq. 5**

$$\mathbf{H}_e \in \mathfrak{H} = \{\mathbf{H}(\phi) \;,\; |\phi - \phi_b| > \alpha\},$$

which means that the eavesdropper is located at a bearing angle that is, at least, away from that of the legitimate receiver, see Fig. 1.

D. Spatial Signature Modulation

In this section, we introduce AoD modulation as a new member of SM family for messages intended for a receiver with a known bearing angle in a LOS MIMO environment. The idea behind AoD modulation is to convey information into the spatial signature of the transmitter antenna array. We introduce the fact that, a transmitter with Nt antennas can arbitrary steer its antenna orientation vector in a sense that, its observed AoD at a certain receiver with known baring angle is recognized at the value intended by the transmitter. The following lemma states this fact formally:
Lemma 1. Let **A** be a transmitter and let **B** be a receiver located in a location known to **A**. Let ϕab be the AoD of **A**'s transmission observed at **B**. Let *yab* be the intended AoD required by **A**, then using the steering matrix

$$\mathbf{S} = diag\left[e^{-j2\pi\frac{d\{\sin(\beta)\}}{\lambda}}\right]_{i=0}^{n-1} \qquad \text{Eq. 6}$$

with β = arcsin(sin(*yab*)+sin(ϕab)) yields the required AoD. Moreover, the described AoD modulation comes with no transmit power cost.
Proof. The first part of the lemma follows by direct substitution with the value of β in **Eq. 7**

$$\mathbf{a}^{\dagger}(\phi_{ab})\mathbf{S} = \left[e^{-j2\pi\frac{d\{\sin(\beta)-\sin(\phi_{ab})\}}{\lambda}}\right]^{n-1}.$$

Meanwhile, the second part of the lemma is found by observing that $S^{\dagger}S = I_n$ and the cyclic invariant property of matrix trace operator. Formally, $tr(SXX^{\dagger}S^{\dagger}) = tr(S^{\dagger}SXX^{\dagger}) = tr(XX^{\dagger})$ and the proof is complete.

The fact elaborated in lemma 1 suggests the use of AoD modulation as a mean for conveying information in the AoD observed at the intended receiver. However, it is not yet clear how beneficial is that sort of modulation from security perspective. Note that the steering matrix, S, in lemma 1, causes the antenna array to go through a uniform rotation as shown in Fig. 2. Therefore, an eavesdropper can infer AoD observed at B from its own observed AoD ; namely, *y*ae. In section III, we will make it clear how AoD modulation can be used to provide positive secrecy rate even if the main channel was degraded with respect to eavesdropper channel.

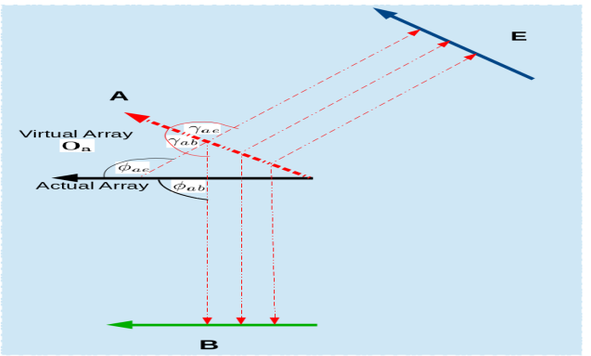

Fig. 2: Rotating the transmitter Antenna Array using the virtual antenna pointing vector Oa

Major Remark:

Note that, the mapping $a^{\dagger}(\phi)\mathbf{S} \rightarrow a^{\dagger}(y)$is a special case of the generalized spatial signature modulation. That is, ULA spatial signature is mapped to another ULA spatial signature. However, this map can generalized to map ULA to any arbitrary spatial signature.

E. Basic Limits of AoD Estimation

The core of the proposed scheme is based on AoD estimation, therefor, we start by introducing the fundamental limits of AoD estimation. In estimation theory, the Cramer Rao Bound (CRB) sets an upper bound on any parameter estimation performance. In particular, it defines the lower bound of the best estimator variance in terms of the solution of the following problem:

Eq. 8

$$\min_{\hat{\theta}(.)} \ \mathbf{var}\left(\hat{\theta}\left(\mathbf{Y}\right)\right)$$

To evaluate the CRB, we start by introducing

Eq. 9

$$\mathbf{U} \models \mathbf{H}^{nlos}\mathbf{X} +$$

where U incorporates all undesired interfering components of the received signal, $1 \leq l \leq L$. Since the receiver objective is to jointly estimate the AoA and AoD of the LOS component, the NLOS diffuse component originated from gorund reflections or scatters from neighboring objects is also considered as an undesired signal. Note that $U\ 100 \sim CN(0_{n\,x\,l}, R_u)$. Accordingly, the posterior distribution of the observation Y is given as follows:

Eq. 10

$$f_{(\mathbf{Y}|H^{los},\mathbf{X})}(\mathbf{Y}) = \frac{1}{\det(\pi\mathbf{R}_u)}\exp\{-(\mathbf{Y}-H^{los}\mathbf{X})^{\dagger}\mathbf{R}_u^{-1}(\mathbf{Y}-H^{los}\mathbf{X})\},$$

which yields the following log-likelihood function **Eq. 11**

$$\mathcal{L}(\mathbf{Y}) = \models \ln\det(\pi\mathbf{R}_u) - \mathrm{tr}\left((\mathbf{Y}-H^{los}\mathbf{X})\mathbf{R}_u^{-1}(\mathbf{Y}-H^{los}\mathbf{X})^{\dagger}\right).$$

Further, It can be shown that, the CRBs of AoD estimation is given by

Eq. 12

$$\mathbf{CRB} = \frac{1}{2}\left[\mathbf{Re}\left(\mu\mathbf{X}^{\dagger}\hat{\mathbf{D}}^{\dagger}\mathbf{G}(\phi)\hat{\mathbf{D}}\mathbf{X}\mu\right)\right]^{-} = \frac{1+k}{2k\mathbf{P}\hat{\mathbf{D}}^{\dagger}\mathbf{G}(\phi)\hat{\mathbf{D}}},$$

$$\hat{\mathbf{D}} = \mathbf{R}_u^{-1/2}\mathbf{D}$$

$$\mathbf{D} = \partial\mathbf{a}/\partial\phi$$

$$\mathbf{G}(\phi) = [\mathbf{I} - \mathbf{a}(\mathbf{a}^{\dagger}\mathbf{a})^{-1}\mathbf{a}^{\dagger}]$$

where the dependence of a on ϕ was dropped for ease of notation. We note that, as $\infty \rightarrow 1$, only LOS component is present and $Ru \rightarrow \sigma^2_N I_n$. Note that, this result is in agreement with that derived in[32]. Also, one can show that (this was also discussed in[32]) efficient estimator exists only asymptotically in the array size for any choice of X that satisfies the power constraint. Looking at the CRB of AoA estimation plotted in Fig. 3 as a function of the true value of AoA,we note that there are some physical interpretations to be made. Signal sources that are closer to the direction of the array axis, i.e. near $-\pi/2$ or $\pi/2$, experience much higher estimation error than those near the direction perpendicular to the array axis, i.e. near zero. Moreover, the Maximum Likelihood (ML) AoA estimator given by:

Eq. 13

$$\hat{\theta}(\mathbf{Y}) = \max_{\theta}\frac{\left|\mathbf{a}^{\dagger}\mathbf{R}_u^{-1}\mathbf{B}\right|^2}{\mathbf{a}^{\dagger}\mathbf{R}_u^{-1}\mathbf{a}} = \min_{\theta}\mathbf{B}^{\dagger}\mathbf{R}_u^{-1/2}\mathbf{G}(\theta)\mathbf{R}_u^{-1/2}\mathbf{B}$$

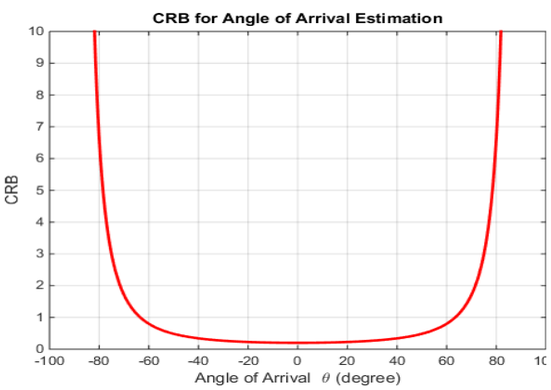

Fig. 3: CRB of AoA estimation assuming ULA configuration.

achieves the CRB with equality asymptotically in the large array size limit, where **Eq. 14**

$$\mathbf{B} = \mathbf{R}_{xy}^{\dagger}\mathbf{R}_{xx}^{-1} \quad \in \mathbb{C}^{n\times 1}$$

$$\mathbf{R}_{xy} \models \frac{1}{L}\sum_{l=1}^{L}\mathbf{X}[l]\mathbf{Y}^{\dagger}[l] \quad \in \mathbb{C}^{1\times n}$$

$$\mathbf{R}_{xx} = \frac{1}{L}\sum_{l=1}^{L}\mathbf{X}[l]\mathbf{X}[l]^{*} \quad \in \mathbb{C}.$$

Furthermore, note that the regularity conditions required for the normality of the ML-AoA estimator holds for the considered model. Thus, in the limit of large sample, the ML-AoA estimator is distributed as a truncated[1] normal distribution by the central limit theorem with mean equals to the true AoA and variance equals to the CRB given in Eq. (12) ([1]the truncation in the normal distribution is due to the finite support of the ML-AoA estimator. We limit the support θ to the interval $[-\pi/2, \pi/2]$ due to the ULA antenna configuration, however, for 2-D antenna configuration with 360° resolution, the support of θ is extended to $[-\pi, \pi]$) . This can be formally expressed as follows:

Eq. 15

$$f_{\hat{\theta}}(\hat{\theta}(\mathrm{Y})) = \frac{1}{\sqrt{2\pi\mathrm{CRB}(\theta_l)}} \frac{\exp\left\{\frac{-(\hat{\theta}-\theta)^2}{2\mathrm{CRB}(\theta)}\right\}}{\Phi\left(\frac{\pi/2-\theta}{\sqrt{\mathrm{CRB}(\theta)}}\right) - \Phi\left(\frac{-\pi/2-\theta}{\sqrt{\mathrm{CRB}(\theta)}}\right)},$$

where ϕ is the cumulative distribution function (CDF) of the standard normal distribution. The results obtained in this section will be useful in the subsequent analysis in the rest of this paper.

III- SPATIAL SIGNATURE MODULATION FOR MIMO WIRETAP CHANNEL

In section II-D, we have introduced AoD modulation as a special case of spatial signature modulation. The major idea therein was to convey the transmitter information into the spatial signature of its own antenna array. In this section, we give the design of the secure modulation scheme designed for the wiretap channel. In its general form, coding for the wiretap channel uses a double layer sequence of codes, inner and outer codes. The inner layer ensures that the transmitted message can be reliably decoded by the legitimate receiver, and the outer layer guarantees that the message is kept secret from the eavesdropper. Following the same convention , in this work, since we are addressing a modulation scheme, we introduce a double layer spatial signature modulation. The inner layer ensures that the transmitter spatial signature can be demodulated reliably at the legitimate receiver. Whereas, the outer layer is designed from multiple random spatial signature in order to assure confusion at the eavesdropper. We give a formal definition of the double layer SSM in the following definition:

Definition 1: Double layer SSM:

Let **A** be a transmitter with a randomly generated antenna orientation vector **O**a, generated according to Lemma 1, kept secret from all other nodes and let **B** be a receiver located at a bearing angle known to **A**. And let **E** be an eavesdropper located in a different geographic location. Let ϕ) be the AoD of **A**'s transmission at **B** after the virtual array rotation.

Then, the double layer SSM is defined as follows:

1- Inner modulation: Inner modulation needs to satisfy:

$$\mathbf{a}^{\dagger}(\phi)\mathbf{W} = \mathbf{a} \qquad \textbf{Eq. 16}$$

2- Outer modulation: Outer modulation is designed as follows:

$$\boldsymbol{W} = \boldsymbol{\Phi}^{-1}\boldsymbol{\Gamma}, \qquad \textbf{Eq. 17}$$

$$\boldsymbol{\Phi} = \boldsymbol{\Pi}(\hat{\boldsymbol{\Phi}}) \qquad \textbf{Eq. 18}$$

$$\boldsymbol{\Gamma} = \boldsymbol{\Pi}(\hat{\boldsymbol{\Gamma}})$$

$$\hat{\boldsymbol{\Gamma}} = \begin{bmatrix} \mathbf{a}^{\dagger}(\beta_1) \\ \mathbf{a}^{\dagger}(\gamma) \\ \vdots \\ \mathbf{a}^{\dagger}(\beta_{N_t-1}) \end{bmatrix}, \qquad \textbf{Eq. 19}$$

where ϕ is an orthogonal matrix in which $a^{\dagger}(\varnothing)$ lies in the same row in which $a^{\dagger}(y)$ lies in $\hat{\Gamma}$, $\beta_i \forall i \in \{1, 2, ..., N_t - 1\}$ are chosen uniformaly at random from (-π, π) and is the row permutation operator.

We note that, ø can be easily generated by the element wise multiplication of elements of $a^{\dagger}(\varnothing)$ with the rows of Hadamard matrix. Also note that, II is unitary, thus, ϕ is also an orthogonal matrix which means ϕ-1 = $\phi^{\dagger}$. Thus, no matrix inversion is needed.

Remark: It is important to note that, probability distribution of W is invariant under the permutation operation of the rows of ϕ and *y*. That is because the rows of ϕ are orthonormal and rows of Γ have the same distribution. Denoting the row index in which $a^{\dagger}(\varnothing)$ and $a^{\dagger}(y)$ reside by $i \in \{1, 2, \ldots, N_t\}$, thus, formally we write **Eq. 20**

$$f_{\mathbf{W}|i}(\mathbf{w}|i) = f_{\mathbf{W}}(\mathbf{w}) \quad \forall i \in \{1, 2, ..., N_t\}$$

This remark is of great importance for the sake of analysis of E's equivocation.

A- Demodulation at **B**

In this section, we describe demodulation of SSM at the legitimate receiver B. The LOS part of the signal received at **B** after SSM reads **Eq. 21**

$$\begin{aligned}\mathbf{Y}^{los} &= \mathbf{H}_b^{los}\mathbf{W}\mathbf{X} + \mathbf{N}_b \\ &= \sqrt{\frac{k}{1+k}}\mathbf{a}(\theta_{ab})\mathbf{a}^{\dagger}(\phi_{ab})\mathbf{W}\mathbf{X} + \mathbf{N}_b \\ &= \sqrt{\frac{k}{1+k}}\mathbf{a}(\theta_{ab})\mathbf{a}^{\dagger}(\gamma_{ab})\mathbf{X} + \mathbf{N}_b.\end{aligned}$$

Note that, Eq. (21) is true for any permutation II for the underlying matrices ϕ and Γ. That is because $a^{\dagger}(\emptyset\ ab)$ and $a^{\dagger}(yab)$ lies in the same row index for any permutation. Therefore, transmitter spatial signature can be demodulated at **B** by simply estimating AoD of the received signal according to Eq. 13. Here, the role of the inner modulation became quite obvious.

B- Demodulation at **E**

In this section, we describe demodulation of SSM at the eavesdropper E. The LOS part of the signal received at **E** after SSM reads **Eq. 22**

$$\mathbf{Z}^{los} = \mathbf{H}_e^{los}\mathbf{W}\mathbf{X} + \mathbf{N}_e = \sqrt{\frac{k}{1+k}}\mathbf{a}(\theta_{ae})\mathbf{a}^{\dagger}(\phi_{ae})\mathbf{W}\mathbf{X} + \mathbf{N}_b.$$

Note that, by the constrain (5) on E's channel, we have $|\phi_{ae} - \phi_{ab}| > \alpha^{\circ}$. Thus, the problem of obtaining the transmitter spatial signature at the eavesdropper is no longer a simple AoD estimation problem as is the case for the legitimate receiver. Rather, the eavesdropper has to estimate transmitter spatial signature from the outer modulation scheme. In the next section, we shall give analysis for **E**'s equivocation considering the outer modulation problem.

IV- SECURITY ANALYSIS OF DOUBLE LAYER SSM

In this section, we study the effect of the proposed double layer SSM on **E**'s equivocation. As pointed out in the previous section, **E** has to extract the transmitter spatial signature from the outer modulation. To analyze **E**'s equivocation, we start by introducing the posterior distribution of **E**'s observation **Eq. 23**

$$f_{(\mathbf{Z}|H_e,W,X)}(\mathbf{z}) = \frac{1}{\det(\pi\mathbf{R}_e)}\exp\left\{-(\mathbf{z}-H_eWX)^{\dagger}\mathbf{R}_e^{-1}(\mathbf{z}-H_eWX)\right\}$$

Note that, **X** and **H***e* are assumed to be known perfectly at the eavesdropper. Thus, it is only left with estimating the spatial signature $a^{\dagger}(yab)$ from its observation. Note that, the posterior distribution of **Z** is independent on the row index *i,* in which the required signature resides. Therefore, The eavesdropper equivocation is lower bounded by its equivocation about the row index, formally **Eq. 24**

$$\mathcal{H}(\gamma_{ab}|\mathbf{Z}) \geq \mathcal{H}(i) = \min\{\log(N_t), C\}$$

where **C** in the capacity of the main channel. This fact leads to the following theorem:

Theorem 1. The Spatial Signature Modulation described in section III achieves equivocation at any eavesdropper having He 2 ∈ ℌ H that is no less than min{log(Nt),C} with equality if and only if the matrix Γ is perfectly recovered from eavesdropper observation.

In fact, the lower bound given by theorem 1 is a loose lower bound. That is because, it does not consider the associated estimation error of Γ. In order to obtain a tighter lower bound, we need to obtain the minimum variance associated with any unbiased estimator $\tilde{\Gamma}_{|}$ (Z) assuming that an unbiased estimator exists.

V- JOINT PHYSICAL-APPLICATION LAYER SECURITY SCHEME

In this section, we introduce the proposed joint physical-application layer security scheme. To establish a secure link over an insecure channel, **A** and **B** are required to agree on a common secret information prior to exchange of confidential messages. Thus, we start this section by introducing the physical layer assisted SKA protocol. A protocol that uses physical layer parameters of the communication channel to turn the completely insecure channel into a physically conditioned secure one. This is done by interpreting the contextual meaning of physical layer parameters into meaningful information that can be used to discriminate legitimate nodes.

In the proposed SKA protocol, a conventional public key based SKA is used to agree on part of the SK. In the same instance, the AoA at the physical layer acts as a defense line against active adversary conditioned on its physical location. In top of the physical layer authentication provided by the AoA information, SSM is done by the transmitter, as explained in section III, is used to generate secret key bits from variations of AoD at the physical layer during the conventional public key based SKA message exchange. Details shall be provided in section VI-A, we will also show that the attacker is kept ignorant of the generated key stream conditioned on its physical location.

Confidential message exchange between A and B in the presence of an active adversary E usually comes with two major requirements:

1- Confidentiality of message contents against E.

2- Message source authenticity since E may be active.

Several cryptographic approaches were proposed to fulfill these requirements. However, in section VI-B we show that the continuous use of AoA information as a mean for message source authentication can be more beneficial. Moreover, AoA is a physical layer information that depend on the respective node locations, thus, node mobility is a major security challenge (as it always was). Therefore, the effect of mobility on the proposed security scheme is also considered.

Before we delve into details of the proposed security scheme, we introduce a useful fact from elementary navigation. In practical communication systems, geographic location are given in the form of GPS coordinates. To check the correspondence between these coordinates and the estimated AoA, the receiver needs first to turn it into bearing information. As shown in Fig. 4, (x_t, y_t) and (x_r, y_r) are the longitude and latitude coordinates of the transmitting and receiving nodes, respectively.

Then, the heading angle, h, measured from the true north of a plane wave emitted at (x_t, y_t) and received at

(x_r, y_r)cab be calculated as follows: **Eq. 25**

$$\theta_h = \arctan(\nu, \upsilon),$$

where:

Eq. 26

$$\nu = \cos(y_r)\sin(x_r - x_t)$$

$$\upsilon = \cos(y_t)\sin(y_r) - \sin(y_t)\cos(y_r)\cos(x_r - x_t).$$

Denoting the angle between the receiver antenna array axis to the true north by θ_r^N, then, the receiver can calculate the expected AoA, θ, of that particular transmitter as follows:

$$\theta = \theta_h + \theta_r^N. \quad \textbf{Eq. 27}$$

Further, in the physical layer, an estimate $\hat{\theta}$ is formed according to Eq. (13) for the actual AoA of the received message. Using the estimate $\hat{\theta}$ from the physical layer and the expected AoA arrival, θ a physical validation of the geographic location of a given node can be made.

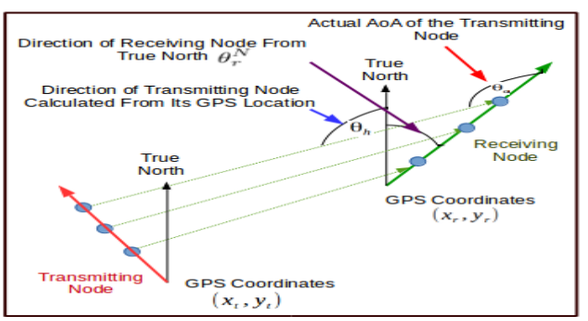

Fig. 4: The relation between the estimated AoA and the bearing information calculated from the GPS location information.

In the next sections, we describe the main components of the proposed joint security framework. First in section VI-A, a novel location aware secret key agreement protocol was adapted, which outputs a location dependent secret key by incorporating the AoA information provided by the physical layer. Then, in section VI-B, we illustrate how the AoA information can enhance the security in a static communication environment. Finally, in section VI-C, we show how the security framework proposed for a static environment can be extended to deal with the possible communication nodes mobility.

VI- FORMULATION OF AOA AUTHORIZATION AS A HYPOTHESIS TESTING PROBLEM

Assuming that the communicating nodes have a prior knowledge of their locations, the problem of deciding whether the received signal is originated from the legitimate physical direction, l, of a given node can be formulated as a two sided hypotheses testing problem as follows:

$$\mathcal{H}_0 : \theta \in \Gamma_0 \quad \textbf{Eq. 28}$$

$$\mathcal{H}_1 : \theta \in \Gamma_1,$$

where Γ0 and Γ1 are the decision regions for $\mathcal{H}0$ and $\mathcal{H}1$, receptively, and are defined as follows:

Eq. 29

$$\Gamma_0 = [-\pi/2, \theta_l) \cup (\theta_l, \pi/2$$

$$\Gamma_1 = \{\theta_l\}.$$

Note that, the probability of misdetection, PMD, which is the probability of rejecting a true $\mathcal{H}1$ hypothesis, will correspond to denying a transmission originated from the legitimate transmitter. Whereas, the false alarm probability of accepting a false $\mathcal{H}0$ hypothesis will correspond to impersonation probability as access will be granted to an illegitimate transmitter.

Recalling the posterior distribution of the received signal given in Eq. 10, we observe that $\mathbf{Y}\|\mathcal{H}_i \sim \mathcal{CN}(H_\theta^{LOS}\mathbf{X}, \mathbf{R}_u)$ where $\theta \in \Gamma_i$ and $i \in \{0, 1\}$. Among different hypothesis testing techniques like Likelihood Ratio (LR), Lagrange Multiplier (LM) or Score tests, the Wald test is the most convenient test for the considered hypothesis testing problem. That is due to the highly nonlinear relation between the observation, **Y**, and the composite parameter we test for, in our case. The Wald test statistics can be found as:

Eq. 30

$$\frac{|\hat{\theta} - \theta_l|}{\sqrt{\mathbf{CRB}(\theta_l)}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \alpha,$$

where, $\hat{\theta}$ is the ML-AoA estimator given in Eq. 13 and is the decision threshold. As noted in section II-E, the CRB of AoA estimation is a function of the AoA as can be seen in Fig. 3 with the fact that angles near the array axis, –π/2 or π/2, experience much higher CRB than those close to zero. Thus, we can notice that the Wald test statistics accounts for that problem by incorporating the CRB to achieve an adaptive decision threshold. Recalling the distribution of the ML-AoA estimator given in Eq. 15, we define both the probability of detection and probability of false alarm as follows:

Eq. 31

$$P_D = P\left(\frac{|\hat{\theta} - \theta_l|}{\sqrt{\mathbf{CRB}(\theta_l)}} \leq \alpha | \mathcal{H}_1\right)$$

$$P_F = P\left(\frac{|\hat{\theta} - \theta_t|}{\sqrt{\mathbf{CRB}(\theta_l)}} \leq \alpha | \mathcal{H}_0\right)$$

Note that under $\mathcal{H}1$, we have $\hat{\theta}$ distributed as given in Eq. 15 with mean equal to θl. Rather under $\mathcal{H}0$, the mean value of $\hat{\theta}$ is equal to the true AoA from which the signal is emitted, θt. Thus, one would expect a relatively high false alarm probability as the attacking node approaches in a close vicinity to the legitimate AoA, θl.

A- Joint Secret Key Agreement Protocol

Symmetric key cryptosystems require transmitting and receiving communication nodes to agree on a secret key prior to communication. The process of sharing the secret key is called Secret Key Agreement (SKA) which can be considered one of the fundamental problems in cryptography. In literature, several scenarios based on the

assumptions about the attacker capabilities, computational power and proactive attitude of the attacker were considered. Public key based SKA protocols (Diffie-Hellman, RSA, Elgamal) are usually based on two assumptions about the attacker:

1-The attacker has a limited computational power.

2-The attacker is pursuing a passive strategy by only eavesdropping the communication link. In[26], Maurer showed that any public key based SKA can be computationally secure rather it can not be unconditionally secure. In the same work, the proposed an information theoretic SKA from public discussion constitutes observing a sequence of realizations of correlated random variables over an insecure channel. In this work, we exploit the AoA as a mean for message source authentication as well as the AoD as a common source of randomness between the communicating nodes from which part of the secret key can be extracted. Moreover, the contextual meaning of those informative physical layer parameters turns the completely insecure channel into a physically conditioned secure channel by introducing the notion of physical hardness. That is an attacker located away from the line connecting the communicating nodes is declared as unauthentic. Thus, a physically secure virtual tunnel between legitimate nodes can be imagined, see Fig. 7.

In this section, we introduce a novel physical layer assisted SKA protocol that leverages the cooperation between smart signal processing techniques at the physical layer and security at the upper layers. As noted before, communication nodes are able to validate their respective physical location using the information provided from signal processing layer as a side information collected during protocol procedures. In addition, we introduce a novel approach for secret key extraction through common randomness without adding extra communication overhead. Assume a SKA protocol that uses C rounds of message exchange to generate a key K of size $|K| = k$ bits at both nodes. We use the modulated AoD of the same C messages, {M1, M2, ..M_C}, exchanged during the public key based SKA to extract a key K_{PHY} of size m bits. Thus, the overall generated key, κ is of size $k + m$ bits. We first start by introducing some basic definitions[26].

Definition 1: SKA protocol consists of C messages is said to be (ϵ, δ) secure against an active eavesdropper whenever it satisfies: **Eq. 32**

$$\mathbf{P}(\mathcal{K} \neq \mathcal{K}') \leq \epsilon,$$

$$\mathbf{I}(\mathcal{K}; Z|\{M_i\}_{i=1}^{C}) \leq \epsilon,$$

$$\mathbf{H}(\mathcal{K}) \geq |\mathcal{K}| - \epsilon,$$

together with that the probability of declaring an active adversary, E, as unauthentic is ≥ 1 - δ at **A** or **B**, ϵ, δ > 0. Before going into details of the proposed SKA protocol, we start by highlighting the protocol structure which can be broken down into three major processes:

1- Conventional public key based SKA.

2- AoA authorization of the received messages.

3- Extraction secret key bits from the AoD which is being modulated by the transmitter.

In the conventional public key SKA, node **A** generate a pair of keys (*Puba, Priva*). To start a secure communication session, **A** sends a request message to **B** asking for its public key accompanied by **A**'s public key. In contrast to the conventional public key based SKA, the physical layer at **B** check the consistence of the received message direction before reply. If the message was originated by **A**, the received message should have arrived through the virtual secure tunnel, otherwise the message is ignored. This physical validation turns the insecure channel into a physically conditioned secure channel as noted before. If the message accepted by **B**, it replies with a response message including its public key, Pubb. The same physical validation is made at **A** which generates the traffic encryption key K and sends it back encrypted with **B**'s public key. The key is accepted at **B** again after the physical validation. Protocol procedures are shown in Fig. 5.

In this section, we introduce a novel approach for extracting secret key bits from a sequence of physical layer observations as a common source of randomness between legitimate communication nodes while keeping the attacker ignorant of the generated key bit stream. Assuming that the angle of the randomly chosen orientation vector and the target AoD are chosen from a uniform distribution ~ (−π /2, π/2), then **Eq. 33**

$$\begin{aligned} H(\gamma_{ab}|\mathbf{Z}) &= H(\mathbf{O}_a|\mathbf{Z}) \\ &= H(\mathbf{O}_a) \\ &= H(\gamma_{ab}) \end{aligned}$$

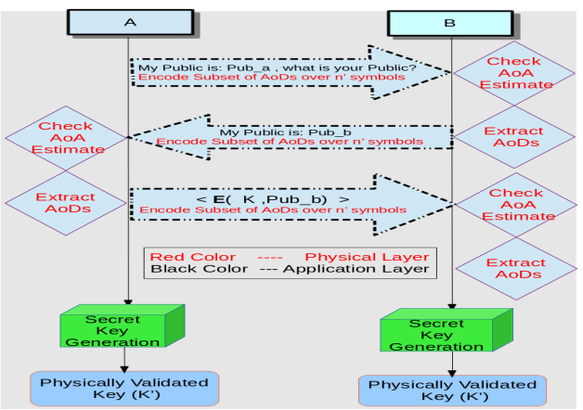

Fig. 5: Procedures of the Proposed Physical layer Assisted Secret Key Agreement Protocol.

Extending Eq. (32) to the vector case that corresponds to v channel uses reads **Eq. 34**

$$\begin{aligned} H(\gamma_{ab}^{v}|\mathbf{Z}) &= H(\mathbf{O}_a^{v}|\mathbf{Z}^{v} \\ &= H(\mathbf{O}_a^{v}) \\ &= H(\gamma_{ab}^{v}) \end{aligned}$$

Where the vector γ_{ab}^{v} can be directly mapped to corresponding m key bits.

B- Confidential Message Exchange in a Static Environment

In a static communication environment, like fixed wireless sensor networks, legitimate communication nodes are distributed over a certain geographic area, each in a certain geographic location. Thus, we assume that nodes **A** and **B** have the location information about each others. Based on this knowledge, each node computes the expected AoA of the transmission of the other node. To establish a secure communication link, nodes **A** and **B** follow the physical layer assisted secret key agreement procedures as pointed out in Section VI-A. At the end of these procedures, the *m* bits of the key extracted from the physical layer together with the *k* bits of the shared session key *K* are used to generate an updated session key, $K' = g(K, K_{PHY})$, where g is an arbitrary function. We point out that, the use of the *m* bits collected from the physical layer is not exclusively dedicated to the generation of an updated session key of same or larger key size. Rather, these *m* bits can be used to provide a more efficient message confidentiality algorithms by an appropriate use in the encryption function itself. We redefine both encryption and decryption functions, $\mathfrak{E}$ and $\mathfrak{D}$ as follows:

$$\mathfrak{C} = \mathfrak{E}(\mathfrak{M}, K') \qquad \textbf{Eq. 35}$$

At the message destination, a physical validation for the actual AoA of the message is made. The receiver forms an estimate, $\hat{\theta}$, according to Eq. 13. Then, it retrieves the original message as follows:

$$\mathfrak{M} = \mathfrak{D}(\mathfrak{M}, K')\,\mathrm{T}(\theta) \qquad \textbf{Eq. 36}$$

where $T(\hat{\theta})$ takes values over {0, 1} according to the result of the Wald test given in Eq. 30.

The encryption and decryption functions defined in this model are based on *K*, K_{PHY}, θa, θ*l*, $\hat{\theta}$ a and $\hat{\theta}$ b, which in turn provide the encryption/decryption function awareness of the legitimacy of the received signal direction. The offered physical layer awareness does not only provide an updated session key, *K*′, but also enable the application layer with the ability to accept or reject a message based on both physical (θa, θ*l*, $\hat{\theta}$ a and $\hat{\theta}$ b) and logical (*K*, K_{PHY}) arguments as opposed to only logical arguments. In a scenario where a fixed communication infrastructure requires a higher level of security, instead of using GPS location information[33, 34] which is susceptible to GPS spoofing attacks[35], the use of AoA estimation can physically insure that only nodes at predefined locations shall be declared as an authentic.

C- Confidential Message Exchange in a Mobile Enviroment

In previous section, legitimate communication nodes, A and B, were assumed static in a given geographic location. This assumption made the pre-sharing of node location information possible. In this section we consider the effect of mobility on the proposed joint security scheme. The core of the proposed scheme is to incorporate the physical location as one of the major security primitives. Therefore, mobility will offer a great challenge as nodes location keep changing over time. Thus, we drop the assumption of the pre-shared location information and the scheme will require communication nodes to share their locations at the beginning of each communication session as well as whenever a communication node moves to another location. While communication nodes movement may be continuous over time, it can be efficiently described by an equivalent discrete time movement model for two reasons:
1-To accommodate the possible estimation error, communication nodes resides within degrees from the expected AoA is considered in the same geographic location.
2-The time scale of the physical movement of a given communication node is much slower than the message exchange rate.

Therefore, without loss of generality, the communication field can be partitioned into sectors within which communication node is considered fixed. Since an AoA estimate associated with any given transmission scans 360^0 the whole communication field

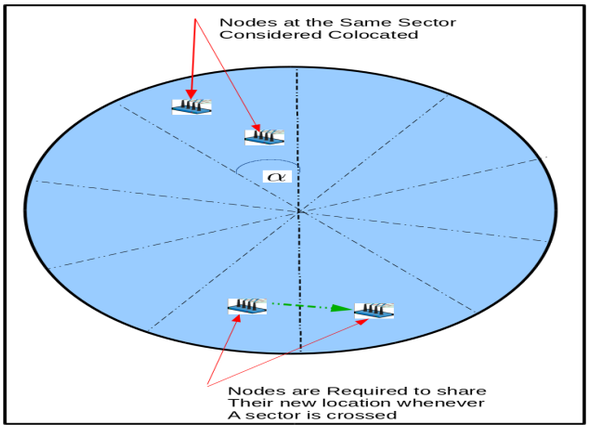

Fig. 6: Dividing the communication environment into 360/α sectors

Whenever a communication node crosses from one sector to another, a physical layer assisted secret key agreement procedures proposed in Section VI-A are required only to share the new AoA estimates (Steps 2 and 3 of the secret key agreement procedures).

This work benefits from the communication nodes mobility as the session key is updated whenever a node crosses from one sector to another. However, this added security comes in the expense of message overhead consumed in the key exchange process.

VII- SECURITY ANALYSIS

In the previous section we introduced the joint physical-application layer security scheme starting from the SK agreement up to the implications of mobility conditions. It is not yet quantitatively clear how the joint work positively affect the overall security performance. The role of this section is to shed the light on the positive effect of such joint work using different security metrics.

We start our analysis by considering the impact of the AoA physical validation on the impersonation probability. We point out that, message decryption and AoA physical validation are done independently. Thus, the overall impersonation probability is defined as the product of the probability of the two independent events. First, the attacker has to brute force all possible values of K' which is of size $k + 2m$ bits. Second, the attacker is either located within α degrees from the line connecting **A** and **B** or the error at the receiver is large enough to realize the attacker transmission direction as authentic. The first event reflects the computational complexity of an encryption function with key size $k + 2m$ bits. Meanwhile, the second event depends on both the attacker geographic location and the target receiver operating characteristics as given in Eq.31. In Figure (7), we introduce the concept of area security where a successful MitM attack requires the attacker to be physically located in the physically vulnerable area shown in figure. Assuming the attacker location to be uniformly distributed over the communication field, the probability that the attacker is located in the physically vulnerable area is given by the ratio between this area and the area of the overall communication field. This can be formulated as follows:

$$\mathbf{P}_I = 2^{-(k+2m)} \times P_{I-PHY}, \quad \textbf{Eq. 37}$$

where **Eq. 38**

$$P_{I-PHY} = P\left(\frac{|\hat{\theta} - \theta_l|}{\sqrt{\mathrm{CRB}(\theta_l)}} \leq \alpha | \mathcal{H}_0\right) \times \left(1 - \frac{A_v}{A_t}\right) + \frac{A_v}{A_t},$$

with A_v and A_t denotes the vulnerable area and total area, respectively. The term P_{I-PHY} given in Eq. 37 quantifies the major advantage offered by the joint physical-application security scheme. It reflects the amount of security amplification earned from the potential cooperation between the physical and application layers. It is clear from Eq. (36) the resiliency against the MitM (which by definition incorporates different types of attacks) is not just weighted by its computational hardness, rather, the contextual meaning of the 2m added bits introduces the notion of physical hardness against such type of attacks.

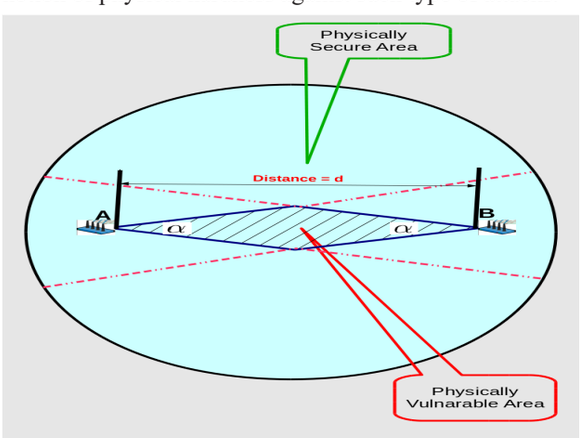

Fig. 7: Dividing the communication environment into physically vulnerable area and secure area.

VIII- CONCLUSION

This paper introduced security architecture that alleviate the cooperation between physical and application layers provides several advantages and unique features that are not available in each paradigm by itself. The problem of exchanging confidential messages between nodes in the presence of an active adversary over an insecure MIMO channel is considered. We introduced the double layer spatial signature modulation (SSM) in which the transmitted information is conveyed into the spatial signature of the transmitting antenna array observed by the intended receiver. Meanwhile, any other eavesdropper does not share the same bearing angle of the legitimate receiver is shown to obtain infinitesimally small amount of information. We also introduced a novel physical layer assisted secret key agreement (SKA) protocol that leverage the cooperation between physical and application layer security. Angle of Arrival and Angle of departure are physical layer parameters that can be exploited not only for their well performance at low SNR, but also for their contextual meaning that provides security advantages. In the proposed SKA protocol, AoA is explored as a physical mean for message source authentication, meanwhile, AoD is used as a common source of randomness in a smart signal processing approach to generate secret key bits without any extra communication overhead. We showed that the eavesdropper can be kept ignorant about the generated key bit stream conditioned on its physical location.

This work introduced the notion of physical hardness to an adversary pursuing either active or passive strategy. We showed that the continuous use AoA as a mean for message source authenticity provides a considerable advantage against active adversary during the message exchange phase. Extending the proposed scheme to a mobile communication environment is also provided. Finally, quantitative analysis for the security gain due the potential cooperation between physical and application layer security is developed.

VIII- REFERENCES

[1] A. D. Wyner, "The wire-tap channel," Bell System Technical Journal, The, vol. 54, no. 8, pp. 1355–1387, 1975.
[2] L. H. Ozarow and A. D. Wyner, "Wire-tap channel ii," AT&T Bell Laboratories technical journal, vol. 63, no. 10, pp. 2135–2157, 1984.
[3] U. M. Maurer, "The strong secret key rate of discrete random triples," in Communications and Cryptography. Springer, 1994, pp. 271–285.
[4] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in Advances in Cryptology-EUROCRYPT 2000. Springer, 2000, pp. 351–368.
[5] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "Ldpc codes for the gaussian wiretap channel," Information Forensics and Security, IEEE Transactions on, vol. 6, no. 3, pp. 532–540, 2011.
[6] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," Information Theory, IEEE Transactions on, vol. 57, no. 10, pp. 6428–6443, 2011.
[7] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth ldpc codes," Information Forensics and Security, IEEE Transactions on, vol. 6, no. 3, pp. 585–594, 2011.
[8] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian mimo wiretap channel," in 2007 IEEE International Symposium on Information Theory. IEEE, 2007, pp. 2471–2475.
[9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part ii: The mimome wiretap channel," IEEE Transactions on Information Theory, vol. 56, no. 11, pp. 5515–5532, 2010.

[10] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," IEEE Transactions on Information Theory, vol. 57, no. 8, pp. 4961–4972, 2011.
[11] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in miso systems with partial channel information," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 704–716, 2012.
[12] D. B. da Costa, N. S. Ferdinand, U. S. Dias, R. T. de Sousa Jr, and M. Latva-Aho, "Secrecy outage performance of mimo wiretap channels with multiple jamming signals," Journal of Communication and Information Systems, vol. 31, no. 1, 2016.
[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Transactions on Wireless Communications, vol. 7, no. 6, pp. 2180-2189, 2008.
[14] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," IEEE Communications Letters, vol. 17, no. 7, pp. 1483–1486, 2013.
[15] ——, "Unshared secret key cryptography," IEEE Transactions on Wireless Communications, vol. 13, no. 12, pp. 6670–6683, Dec 2014.
[16] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in mimo wiretap channels," IEEE Transactions on Communications, vol. 61, no. 1, pp. 144–154, 2013.
[17] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of tas/mrc with antenna correlation," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 254–259, 2013.
[18] S. Shafiee and S. Ulukus, "Achievable rates in gaussian miso channels with secrecy constraints," in 2007 IEEE International Symposium on Information Theory. IEEE, 2007, pp. 2466–2470.
[19] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," IEEE Journal of Solid-State Circuits, vol. 43, no. 12, pp. 2674–2692, 2008.
[20] Y. Ding and V. F. Fusco, "Mimo-inspired synthesis of directional modulation systems," IEEE Antennas and Wireless Propagation Letters, vol. 15, pp. 580–584, 2016.
[21] ——, "A vector approach for the analysis and synthesis of directional modulation transmitters," IEEE Transactions on Antennas and Propagation, vol. 62, no. 1, pp. 361–370, Jan 2014.
[22] M. Hafez, T. Khattab, T. Elfouly, and H. Arslan, "Secure multiple-users transmission using multi-path directional modulation," in Communications (ICC), 2016 IEEE International Conference on. IEEE, 2016, pp. 1–5.
[23] Y. Ding and V. Fusco, "Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters," IEEE Antennas and Wireless Propagation Letters, vol. 14, pp. 1330–1333, 2015.
[24] ——, "Constraining directional modulation transmitter radiation patterns," IET Microw., Antennas Propag, vol. 8, no. 15, pp. 1408–1415, 2014.
[25] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," arXiv preprint arXiv:1606.04488, 2016.
[26] U. Maurer, "Information-theoretically secure secret-key agreement by not authenticated public discussion," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1997, pp. 209–225.
[27] A. Kitaura, H. Iwai, and H. Sasaoka, "A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio," in The 9th International Conference on Advanced Communication Technology, vol. 3, Feb 2007, pp. 1763–1767.
[28] X. Sun, W. Xu, M. Jiang, and C. Zhao, "Improved generation efficiency for key extracting from wireless channels," in 2011 IEEE International Conference on Communications (ICC), June 2011, pp. 1–6.
[29] O. Gungor, F. Chen, and C. E. Koksal, "Secret key generation via localization and mobility," IEEE Transactions on Vehicular Technology, vol. 64, no. 6, pp. 2214–2230, June 2015.
[30] A. Badawy, T. Khattab, T. El-Fouly, A. Mohamed, D. Trinchero, and C.-F. Chiasserini, "Secret key generation based on aoa estimation for low snr conditions," in 2015 IEEE 81st Vehicular Technology Conference (VTC Spring). IEEE, 2015, pp. 1–7.
[31] A. Badawy, T. Elfouly, T. Khattab, A. Mohamed, and M. Guizani, "Unleashing the secure potential of the wireless physical layer: Secret key generation methods," Physical Communication, vol. 19, pp. 1–10, 2016.
[32] J. Li, B. Halder, P. Stoica, and M. Viberg, "Computationally efficient angle estimation for signals with known waveforms," IEEE Transactions on Signal Processing, vol. 43, no. 9, pp. 2154–2163, Sep 1995.
[33] R. Hussain, F. Abbas, J. Son, and H. Oh, "Tiaas: Secure cloud-assisted traffic information dissemination in vehicular ad hoc networks," in Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on, May 2013, pp. 178–179.
[34] D. E. Denning and P. F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," Computer Fraud & Security, vol. 1996, no. 2, pp. 12–16, 1996.
[35] M. S. Al-kahtani, "Survey on security attacks in vehicular ad hoc networks (vanets)," in 2012 6th International Conference on Signal Processing and Communication Systems (ICSPCS), Dec 2012, pp. 1–9.