Reduction of Secondary Lobes in Joint angle and Delay Estimation in Angle of Arrival Localization to Detect MAC Address Spoofing in Wireless networks

Sara Adel[1] and Eman Mohammed[2]

[1]Department of Information Technology, Faculty of computer and information science, Mansoura University, Egypt
[2] Department of Information Technology, Faculty of computer and information science, Mansoura University, Egypt

***Abstract*:** in this paper, we solve the problem of secondary obes that are due to noise that comes from constructive and destructive multipath interference that are resulted in received signal strength (RSS) variation over time. This is to develop a very efficient localization algorithm that uses a unique fingerprint of angle of arrivals (AOAs) , in a specified range, with associated time delays (TDs), in the surrounded sparsity design promoting multipath parameter (i.e:RSS). We solve this problem to detect physical identity spoofing of nodes in radio wireless networks, and localize adversaries and jammers of wireless networks. All radio waves are vulnerable to many types of attacks due to the ability to capture them and sniff or eavesdropping on them in the open space. Physical identity spoofing is used to launch many types of attacks against wireless networks like Denial of Service (DOS), Man-In-The-Middle and Session Hijacking and eavesdropping. Eavesdropping is a human-based social engineering attack. Active adversaries are able to jam and eavesdrop simultaneously, while passive adversaries can only eavesdrop on passed signals. In TCP/IP protocol for example, Media Access Card (MAC) Address is transferred in 802.11 frames. Detection process was carried out by analyzing electromagnetic radio waves that are used to transfer data, in the form of radio wave signals that are formed by the modulation process which mixes the electromagnetic wave, with another one of different frequency or amplitude to produce the signal with a specified pattern of frequency and amplitude. We depended on the angle of arrival of vectors and time delay across scattered areas in the surrounded space to solve the problem of co-location in detection and localization of jammers. We used Maximum Likelihood (ML) angle of arrival determination because Maximum Likelihood approaches, known to their higher accuracy and enhanced resolution capabilities. And we assessed their computational complexity that was considered as the major drawback for designers to their implementation in practice. Our solution was tested on a jammer that changed the signal strength of received signal at the receiver at an angle of arrival 30 degree. And we used scatterers density to determine the angle of arrival of the sender. The simulation has observed that the power of the received signal has changed from the range of angles 20 to 40 degrees. We used scatterers because they describe the density of the signal power, and also enhance the signal to noise ratio, that resulted from the multipath fading of the signal strength. And also overcoming the problem of secondary lobes that are due to signal propagation, while determining the angle of arrival of a signal sender. So, we developed a new passive technique to detect MAC address spoofing based on angle of arrival localization. And assessed the computation complexity of the localization technique through depending on a range angle to estimate the angle of arrival of the adversary within it. And we reduced number of secondary lobes, and their peaks, in the importance function, while determining the angle of arrival, and so increasing the accuracy of angle of arrival measurement. We compared our work to other techniques and find that our technique is better than these techniques.

***Keywords*:** Physical identity address spoofing detection, radio waves, wireless networks, data signal formation and pattern, power delay spectrum and beam width

1. Introduction

The media access control (MAC) address identifies wireless devices in wireless networks, so it can be used in identity-based attacks. MAC address spoofing is an attack that changes the MAC address of a wireless device that is in a specific wireless network, using off-the-shelf equipment. An attacker can spoof the MAC address of an access point (AP) in WLAN-infrastructure mode and replace or coexist with that AP to eavesdrop or make jamming on the wireless traffic or act as a man-in-the-middle. Also the attacker can flood the network with numerous requests using random MAC addresses to exhaust the network resources. Many methods and researches have been proposed to detect the problem of MAC address spoofing, as in [1] and [2]. In [1] they detected the spoofing attack and localize the adversary. From [3], there are two main types of device localization. The first type is Model-based localization, in which a reference propagation model is used, and localization is depending on received power at a reference distance d_0 from the transmitter. And the second type is Fingerprint-based localization, in which the problem of localization is tackled as a classification problem, where each location corresponds to a different class. Our new solution to detection problem depended on solving the problem of co-location in Fingerprint-based localization, such that increasing the accuracy of detection and localization, by means of vectors of angle of arrival of signal components that are local scatterings that occur in proximity to T_x/R_x antenna [4], and spatial consistency [5]. Spatial consistency is obtained by environment pattern that contains the most effective geometry information. So this environment pattern is useful for generating integral and accurate channel geometry. In MAC address spoofing, spoofed frames are sent out, by the adversary's rogue device, with spoofed media access card address, resulting in congestion in the network from the quality of service (QOS) and throughput point of view as in [6] and [7], and change in the signal pattern of original legal signal in the physical medium [1]. But for the adversary to know the legal physical identity and spoof it, he firstly must passively sniff on the traffic passing in the propagated signal that is broadcasted in the open and diverse wireless medium space, between a transmitting source of modulated electromagnetic wave, and the destination [6]. And as discussed before, in passive sniffing, the adversary only can eavesdrop on transmitted data, but in active sniffing, the adversary can eavesdrop and jam simultaneously.

Each wireless antenna is emitting electromagnetic waves that represent frames, with a specified pattern of the field radiated

by this antenna. The pattern is essentially formed from the radiation characteristics of the antenna itself. Signal strength of a frame means the power level at which this frame can be received at the destination (antenna). We can use this signal pattern to detect and localize the adversary because MAC address spoofing is resulted in many attacks like ARP-DNS-web spoofing- Email spoofing as in [8].and we can guarantee a full secured system if we ensured the security of it's physical layer. We found that the best way to detect this problem is analyzing the direction of arrival of signal and its vector pattern. We define some of the common notations that will be adopted in this paper, as in [9] where $\{.\}^{T}$ and $\{.\}^{H}$ denote the conjugate and Hermitian (i.e. transpose conjugate) operators. And as in [6], the transmitted signal from legitimate transmitter and its covariance matrix are denoted by Z_s and $G_s = E\{ZZ_s^H\}$ respectively, with normalized transmit power constraint for this legitimate transmitter, $\{G_s: \ G_s \geq 0, \ tr(G_s)\}$ where ρ_s is the maximum tolerable transmission power for it. And the transmitted signal from the active adversary q to destination and its covariance matrix are denoted by Z_{q1}, and $G_{q1} = E\{Z_{q1}Z_{q1}^H\}$ respectively, with normalized transmit power constraint for this adversary, $\{G_{q1}: G_{q1} \geq 0, \mathrm{tr}(G_{q1} \leq P_q\}$, where ρ_q is the maximum tolerable transmission power for it. In [4], they discussed that determination of angle of arrival in the form of distribution is not impossible but the limitation of measurement of discreteness of angle is resulting from limited width of receiving antenna beam. So modeling local scatterers in the surrounded area of cube like in [5] is very essential to observe local scatterer distribution, by means of significant scatters. Significant scatterers are scatterers that have power greater than a specified threshold [5]. So if we specify a threshold taken from the surrounded environment, such that this threshold differentiates between the presence of an attack from legal transmission, we would detect the presence of anomalies. And if we specify the surrounded are of the receiver as a cube, its width W_D is defined by the environmental pattern, as it is the range of **significant scattered** multipath components along the y-axis of the cube as in figure 1. Y-values can be obtained randomly over W_D using uniform discrete probability density function.

Note that in [5], they dealt with the surrounding area of transmitter but here we dealt with the surrounding area of receiver to detect the adversary that launches the attack on the receiver. The position of the scatterer is given as $[x_q, y_q, z_q]$, where $q = 1,..., N_{sca}$ and N_{sca} is determined by density x_Q i.e., the number of scatters per cubic meter, and the cube volume. This cube width in space can be used to accurately selecting the sparsity-promoting design parameter ρ_1 that was discussed in [9]. And so we could reduce secondary lobes while obtaining the angle of arrival of these scatterers that are propagated randomly. And so estimation of number of paths that are depended mainly on sparsity feature that is inherent to marginal delay, $\bar{g}_{\bar{\tau}}(\tau_i)$ so that we can get time delay estimates from it as was discussed in [9], when a signal hitting multiple receiving antennae in a homogeneous environment.

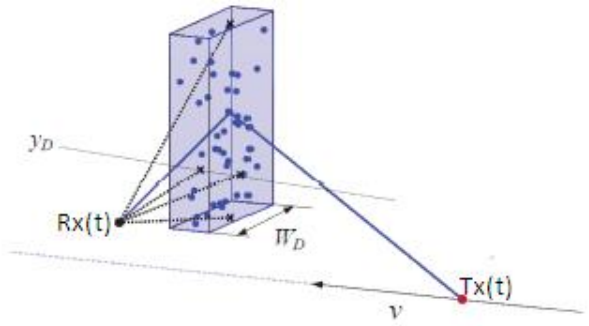

Figure 1. Geometrical illustration of the scattered multipath Component

In [9], they tackled the problem of joint angle and delay estimation through multiple reflections of a known signal hitting multiple receiving antennae, and they showed that the localization performance was below 15 cm accuracy,but the computation complexity was the main drawback in implementation of the localization technique. In [3] they showed that a distinctive fingerprint for localization can be defined as the vector of RSSI values, and in [7], the detection process depended on observing the effect of the spoofing attacks on the quality of service (QOS) of the network and data rate of spoofed frames flooding. The challenge was that there is no verification mechanism for the nodes' physical addresses. When we looked at the signal pattern as an area that is formed from spatial points, the Point is considered to be an arbitrary location within an area, and the Event is the observation of this location. The signal strength variation between different points in a specified area is studied as a Mapped Point Pattern, to make a continuous spatial tracing, such that all relevant events were recorded by means of vectors, and the anomalous events were recognized according to spatial continuity analysis.

An attacker can spoof the MAC address of a legitimate wireless device to hide his/her identity to deny service on a given wireless network [6].

In the IEEE 802.11 standards, it is necessary to exchange the four-way handshake frames before an association takes place between a wireless device and the AP. Once the station is associated with the AP, a hacker can disturb this association by sending a targeted deauthentication/disassociation [7] frame to either disconnect the AP by spoofing the MAC address of the wireless user or disconnect the wireless user by spoofing the MAC address of the AP, or sending frames to all of the wireless users using a broadcast address by spoofing the MAC address of the AP. After sending the frame, the AP or the user who receives the frame is disconnected and has to repeat the entire authentication procedure in order to connect again. The attacker can also send spoofed deauthentication frames repeatedly to prevent the wireless user or the AP from maintaining the connection [8].There are also other attacks, such as jamming.

The attacker can spoof the MAC address of any device in the network, either as a wireless device or the AP. Then he/she can change his/her transmission power, and sends a jamming signal to the reciever. Our aim is similar to [9], which is to detect the jammer by localizing the legitimate wireless

device and rouge device, using RSS samples. We assume that a receiver legitimate station is not mobile. In the jamming period, we can actively send packets to a legitimate device to show scatterrers in RSS samples to measure the angle of arrival. We can detect the attacker if two different locations are returned for the same MAC address.

There are some limitations in the previous work. Sequence number approaches suffer from some drawbacks: control frames don't have any sequence number at all, spoofing of control frames is possible. Furthermore, some of the tools used by the hackers provide the capability of eavesdropping and injecting frames that have sequence numbers similar to the frames of the legitimate device. OS fingerprinting techniques have some weaknesses, like that data frame only can be detected by the network layer's OS fingerprinting. Another weakness is that some of the detection techniques assume that the attacker spoofs the MAC address using Linux-based operating system tools. This assumption could cause some attackers to bypass the intrusion detection system. The attackers can use a capability that the Windows operating system provides to change the MAC address of a given user. Finally, vendor information, capability information and other similar fingerprinting techniques can be easily spoofed using off-the-shelf devices. Reccieved signal strength approaches depended on making localization according to the signal strength that is variated due to propagation in the environment. When the attacker and the victim devices are close to each other, the means/medians of both devices are close to each other, so distinguishing the two devices becomes hard. Furthermore, the distribution of the data from a single device can construct two clusters, so it is hard for the clustering algorithm-based approaches to perform well. The purpose is finding a balancing point at which a smaller set of features that let the system to be capable of accurately detecting the node of interest.

2. Related Work

2.1 Localization through received signal strength:

A previous work in [2], depended on lognormal distribution `of received signal and matching it to the location through the degree of RSS correlation, according to the central tendency of received signal strength values to the medoids of one of two classes, as the aim was to find out the spatial distance in signal (power strength) space between the presence of a spoofing adversary and ordinary legal wireless signal strength. This is determined according to the spatial correlation in signal power strength between spatial points in space which is called by spatial continuity analysis. The main problem is that this correlation is calculated upon the environmental factors affecting the wireless propagated signal. And the main idea of detection depended on cluster analysis by using Partitioning Around Medoids (PAM) method as it was more robust in the presence of noise and outliers, compared to the popular k-means method. In PAM method, spoofing detection depended on spatial correlation between received signal strength, and measured received signal strength, at landmarks, with known reference locations. The received signal strength was considered as test statistic on the distance between two medoids of two partitioned clusters for each node identity, which are legal class cluster and spoofed class cluster.

2.2 Signal strength interpolation

In [10], they depended on interpolating the signal strength values to produce an estimated surface of signal strength values, by using kriging method that takes some known signal strength values of points spaced by a specified distance. But kriging mainly models the spatial structure of measured points to give the estimated surface, according to the specified distance between these measured points. And in [11] for localization, the method of radio frequency fingerprinting-based localization depended on designing datasets containing features that are selected from the RF signal characteristics, in different locations. To form a location fingerprint database, the problem is that it requires forming a tedious site survey that maps RF signals with the physical environment. This requires quite and accurate feature selection for making accurate fingerprints by the selected features. Then testing the fingerprints of RF signals, at random locations in the surveyed area. The signal data would be input to the localization System that uses a classification algorithm, to see the accuracy of finding the true locations of these random fingerprints. The process of producing a fingerprint database on a radio map requires a user to manually tell the system where they are, so that the system can learn the RF signal pattern at that specific location. This is very tedious and time-consuming. And if few features are used to build the fingerprints, the training time and classification time for the machine learning algorithm can be shorter. This is good for real time classification. But fewer features resulted in the difficulty of finding fingerprints that would be unique enough for the localization process. And so higher classification error would be resulted. So the challenge is finding a balancing point at which a smaller set of features that let the system to be capable of accurately detecting the node of interest. The disadvantage of this method is the probability that two locations may be of similar signal pattern.

2.3 Localization through angle of arrival

As discussed in [9], where the reception angle estimation was through joint angle and delay estimation, the system model was for a transmitted signal modulated over M+1 sub carriers. After undergoing multiple reflections, it impinges on the receiving antennae array from $\bar{Q}$ different Angles $(\overline{\alpha}_1, \overline{\alpha}_2, ..., \overline{\alpha}_Q)$, with associated time delays $(\overline{T}_1, \overline{T}_2, ..., \overline{T}_Q) \subset [0, T_{max}]^Q$, where T_{max} can be as large as desired. And the channel estimates across all antenna elements at each m^{th} sub carrier into a single vector,

$$h(m) = [h_1(m), h_2(m), ..., h_p(m)]^T, \quad (1)$$

$$h(m) = \sum a_m(\overline{\alpha_q})\overline{\gamma_q} e^{j2\pi m \Delta f \overline{T_q}} + w(m) \quad (2)$$

Where $w(m) = [w_1(m), w_2(m), ..., w_p(m)]^T$ (3), is the corresponding noise vector, and $a_m(\alpha) \underline{\Delta} [e^{j2\pi_{1,}, m(\alpha)}, e^{j2\pi_{2,m(\alpha)}}, ..., e^{j2\pi_{p,m(\alpha)}}]^T$ (4), is the array steering vector defined for any direction α, and $\bar{\gamma}_q$ is constant coefficients across all the sub carriers and antenna elements.

And as discussed in [2], the detection depended on the distance between two main medoids of clusters, taking into consideration the parameters of transmission power levels, and distance between spoofing node and original node, and then classifying the multiple number of adversaries into classes. But the main problem with machine learning classification and previous solutions was co-location in which two or more users are in the same place [3].

2.4 Localization through random forests

In [12], they used random forests to make the localization. But signal attenuation that was because of several factors, such as multi-path fading and obstacles that made the signal oscillate, especially when there is a significant distance between the sender and receiving device, and they depended firstly on building a profile of the legitimate device to develop characteristics of normal behavior, assuming that there is no attacker at the stage of building a profile. And this was the first drawback of this solution. The second drawback was that they depended on the fact that RSS samples at a specific location are similar while the RSS samples at two different locations are distinctive, and this is not achieved in all cases because as said before, in section 2.2, two different locations may be of similar signal pattern. And they depended on a machine learning algorithm that requires high set of features, and so higher time consuming, and as said before in section 2.2 the challenge is finding a balancing point at which a smaller set of features that let the system to be capable of accurately detecting the node of interest.

3. MAC Address Spoofing Detection by Localization through Angle of Arrival Determination by using Scatterers

In [4] they depended on clustering of signal components or parameters to estimate angle of arrival distribution. These parameters are defined on the basis of power delay spectrum (PDS) selected points. And they depended on using multiellipical model of delayed scattering component and von Mises' power delay profile (PDP) for local scattering components, but we depended in obtaining the angle of arrival to locate the adversary, on modeling scattered multipath components, and this can be achieved by observing the distribution of scatterers and their geometry, and using the transfer function of amplitude of scatterers [5] as follows.

$$H_{Sca}(t,f) = \frac{c}{4\Pi f d_{T,q} d_{R,q}(t)} S(t,f).e^{j\varphi q} \quad (5)$$

Where $d_{T,q}$ is the time-invariant distance between T_x and the q^{th} scatterer, and $d_{R,q}(t)$ is the time-varying distance between $R_x(t)$ and the q^{th} scatterer, and $s(t,f)$ refers to the scattering coefficient and φt is the random phase modeled by a uniform distribution over [0, 2π).

The amplitude of the transfer function is divided into a distance-dependent part, and a scattering coefficient part. So after subtracting the distance-dependent part, the scattering coefficients are evaluated for individual time Instants. It was found that the PDFs of $s(t,f)$ at different times can be modeled well by the Gaussian distribution, by which the mean values and standard deviations can be estimated using the nonlinear least squares regression method. So, the PDF of the time-varying scattering coefficient is given as:

$$f(s(t,f)) = \frac{1}{\sigma_s \sqrt{2\pi}} \exp\left(- \frac{\left(S(t,f) - \mu_s(t,f)\right)^2}{2\sigma_s^2} \right) \quad (6)$$

Where $\mu_s(t,f)$ is the mean value at time t for frequency f. In [4], they discussed that the problem is that **no one** geometric model is best by all criteria and for all environments. Because no definite relationship can explicitly associate the parameters of distributions of azimuth and elevation angle, with different types of propagation environments and the distance between the transmitter (Tx) and the receiver (Rx).

But geometric channel model (GCM) can give the possibility of calculating the impact of changes in the position of the objects (TX, Rx), on the spatial properties of the received signals due to the propagation environment type. And the parameters of the GCMs are defined on the basis of the PDS or PDP and the relative position of the transmitter and the receiver. This is because they reproduce the geometry of the spatial relationships among TX, Rx, and the location scattering areas with their spatial density and these criteria differentiate the individual models. And so they provide the basis for theoretical analysis of PDFs of AOA through a statistical model of AOA which is a PDF estimator that is closely related to the type of propagation environment that has temporal characteristics of transmission channel.

4. Determining Angle of Arrival through Receiving Antenna Beam Width to overcome Co-location problem

Since the idea is that we can detect the Mac address spoofing through the signal strength of frames emitted from a specified node's Network Interface Card (NIC), then we have looked at the antenna pattern as a group of vectors representing the signal strength and frequency, and the direction of the field received from an antenna. But due to the broadcast nature of signals in wireless medium, and the attenuation that comes out from obstacles that face the signal in the broadcasting medium, the power and direction can be varied. The signal can be exposed to diffraction, scattering, reflection, transmission, and refraction while propagation [13], but because each sending device has it's signal and due to the propagation pattern which can be considered as a fingerprint relating the signal at scattered regions surrounding the receiving node , spoofing detection can be possible if a gap difference in received signal strength of frames with the same Mac address exceeds a specified threshold determined from the spatial continuity analysis and correlation structure of signal propagation in the physical environment in which the signal is broadcasted. We have used Beam forming as in [14], [15] and [16] and the concept of vectors in [9] to determine the directionality of' a signal and so sensitivity from it's radiation pattern.

As was discussed in [14], Directional beam forming (BF) transmissions using antenna arrays overcome the difficulty of high signal attenuation and mobility effect of moving devices and their orientation, and body shadowing. And as

discussed in [4] about local and delayed scatterers and that their locations, that we can determine from them, the position of TX and RX which are located at a distance D So we have showed directional gain antennas when receiving a stream of spoofed frames, the radiation pattern that changed the pattern of the legal sending node, over time to detect the presence of the adversary as well as localizing it. In [9], estimation of number of paths depended mainly on sparsity feature that is related to marginal delay, $\bar{g}_{\bar{\tau}}(\tau_i)$ that we can get time delay estimates from it. So by accurately selecting the sparsity- promoting design parameter ρ_1, as in [9], and depending on scatterers density and that is also mainly related to path loss characterization in [17] and signal strength attenuation as in [12], we could depend on local scatterers, without depending on signal strength interpolation, so we could reduce the secondary lobes that are due to noise contribution and so reducing the mean square error in equation (5) and (6). Because the role of this design parameter is controlling the spans of main lobes that appear around the true unknown angle of arrivals and time delays. And the parameter ρ_0, that it should be sufficiently high value that is optimized offline according to observed behavior of estimator, as discussed in [9]. We depended on scatterers that defined directionality and gain to make the detection and localization more accurate, in the surrounded scattering areas as in [9], and showed how the distance between transmitter and receiver affected the amplitude of the signal as discussed in [9] and [5]. And so we showed results with the concept of pointing and beamwidth. And we have introduced representative sampling in [18], instead of random windowing, on multiple trace files, to improve coherence discovery in cross spectral density in [19], so that forming links and paths by the number of sampled units taken from the coherent subset. The size of the coherent subset, and inclusion probability that gives the sample size and Depending on the distance function that can calculate the distance between population units in general auxiliary spaces to capture the pattern characteristics. And in [15], the beam is formed at any time n, as y (n) which is a linear combination of the data from M antennas, with x (n) being the input vector and w (n) is the weight vector.

$$Y(n) = w^H(n) * x(n) \quad (7),$$

Where weight vector $W(n)$ can be defined as:

$$w(n) = \sum_{n=0}^{M-1} wn \quad (8)$$

And input vector $x(n)$ can be defined as

$$x(n) = \sum_{n=0}^{M-1} Xn \quad (9)$$

In [9], it was discussed that the approximate concentrated likelihood function (CLF) decomposition which is the superposition of the separate contributions pertaining to the $\bar{Q}$ angle-delay pairs, to be separable in terms of the angle-delay pairs as originally required.

We can use the equation of PDF of time varying scattering coefficient, (equation (6)), instead of the part of the periodogram of the signal that was discussed in the CLF equation that was equation (38) in [9], as follows:

$$\varsigma_c \approx \frac{1}{P(M+1)} \sum_{q=1}^{\bar{Q}} I(\alpha_q, \tau_q) \quad (10)$$

Where $I(\alpha_q, \tau_q)$ is the periodogram of the signal given by:

$$I(\alpha,\tau) = \left| \sum_{p=1}^{P} \sum_{m=-M/2}^{M/2} e^{-j2\pi\varphi p,m(\alpha)} h_p^*(m) e^{-j2\pi wm} \right|^2 \quad (11)$$

In which (m) is the p^{th} element of the vector h (m)

And the factor $\frac{1}{P(M+1)}$ is absorbed in the new design parameter, $p_1 \neq p_0$.

And after exploiting the approximation of the above CLF as **importance function** (upon normalization) which is equation (40) in [9] as:

$$\bar{\varsigma}(\alpha,\tau) = \frac{\exp\left\{ p_1 \sum_{q=1}^{\bar{Q}} I(\alpha_q, \tau_q) \right\}}{\int \ldots \int \exp\left\{ p_1 \sum_{q=1}^{\bar{Q}} I(\alpha_q', \tau_q') \right\} d\alpha' d\alpha'} \quad (12)$$

And after factorizing it in equation (41) in [9], to be separable in terms of the angle-delay pairs as originally required as follows

$$\bar{\varsigma}(\alpha,\tau) = \prod_{q=1}^{\bar{Q}} \bar{g}_{\bar{\alpha},\bar{\tau}}(\alpha_q, \tau_q) \quad (13)$$

So, we could carefully design the importance function, and compute time delays and angles of arrival expectations at any desired degree of accuracy, by increasing number of realizations using the corresponding sample mean estimates, as it would be discussed, but in a defined range of angles, where,

$$\bar{g}_{\bar{\alpha},\bar{\tau}}(\alpha,\tau) = \frac{e^{p1I(\alpha,\tau)}}{\int\int e^{p1I(\alpha',\tau')} d\alpha' d\tau'} \quad (14)$$

Is a common private distribution for all angle-delay pairs. So vector realizations $\alpha^{(r)} and \tau^{(r)}$ can be generated using the multidimensional distribution $\bar{\varsigma}(\alpha,\tau)$ by generating $\bar{Q}$ independent couples (α_q^r, τ_q^r) using $\bar{g}_{\bar{\alpha},\bar{\tau}}(\alpha,\tau)$ then constructing $\alpha^{(r)} = [\alpha_1^{(r)}, \alpha_2^{(r)}, \ldots \alpha_{\bar{Q}}^{(r)}]$ and $\tau^{(r)} = [\tau_1^{(r)}, \tau_2^{(r)}, \ldots \tau_{\bar{Q}}^{(r)}]$, by factorizing the joint distribution $\bar{g}_{\bar{\alpha},\bar{\tau}}(\alpha,\tau)$ as the product of marginal and conditional pdfs, in two equivalent forms, as equations (49) and (50) in [9] as follows:

$$\bar{g}_{\bar{\alpha},\bar{\tau}}(\alpha,\tau) = \bar{g}_{\bar{\tau}}(\tau)\, \bar{g}_{\bar{\alpha}|\bar{\tau}}(\alpha \mid \tau) \quad (15), \text{ and}$$

$$\bar{g}_{\bar{\alpha},\bar{\tau}}(\alpha,\tau) = \bar{g}_{\bar{\alpha}}(\alpha)\, \bar{g}_{\bar{\tau}|\bar{\alpha}}(\tau \mid \alpha) \quad (16)$$

Where $\bar{g}_{\bar{\tau}}$ [resp., $\bar{g}_{\bar{\alpha}}(\alpha)$] is the marginal pdf of τ [resp. α] and $\bar{g}_{\bar{\tau}|\bar{\alpha}}(\tau \mid \alpha)$ [resp., $\bar{g}_{\bar{\alpha}|\bar{\tau}}(\alpha \mid \tau)$] is the conditional pdf of τ given α [resp., α given τ]

Then we can generate the required realizations through the following two alternatives:

1) Alternative 1: generating $\tau_q^{(r)}$ using $\bar{g}_{\bar{\tau}}(\tau)$ and then using $\bar{g}_{\bar{\alpha}|\bar{\tau}}\left(\alpha \mid \tau = \tau_q^{(r)}\right)$ to generate $\alpha_q^{(r)}$

2) Alternative 2: generating $\alpha_q^{(r)}$ using $\bar{g}_{\bar{\alpha}}(\alpha)$ and then use $\bar{g}_{\bar{\tau}|\bar{\alpha}}\left(\tau \mid \alpha = \alpha_q^{(r)}\right)$ to generate $\tau_q^{(r)}$

But we selected the first alternative as it was discussed in [9], that the second alternative would be not good option since $\bar{g}_{\bar{\alpha}}(\alpha)$ can't allow resolution of closely-spaced angles. And $\bar{g}_{\bar{\tau}}(\tau)$ is able to resolve closely-spaced delays even if the two paths are also extremely closely spaced in the angular domain and it always exhibits $\bar{Q}$ main lobes around the true unknown time delays (TDs), $\{\bar{\tau}_q\}_{q=1}^{\bar{Q}}$, and after evaluating $\bar{g}_{\bar{\tau}}(\tau)$ as equation (51)in [9],as follows:

$$\bar{g}_{\bar{\tau}}(\tau) = \int \bar{g}_{\bar{\alpha},\bar{\tau}}(\alpha,\tau)d\alpha \quad (17)$$

This is then used to generate r^{th} vector of delay realizations $\tau^{(r)} = [\tau_1^{(r)}, \tau_2^{(r)}, \ldots \tau_{\bar{Q}}^{(r)}]^{\tau}$, then each $\{q^{th}\}_{q=1}^{\bar{Q}}$ conditional angle pdf in equation (52) in [9] as:

$$\bar{g}_{\bar{\alpha},\bar{\tau}}\left(\alpha \mid \tau = \tau_q^{(r)}\right) = \bar{g}_{\bar{\alpha},\bar{\tau}}\left(\alpha, \tau_q^{(r)}\right) / \bar{g}_{\bar{\tau}}\left(\tau_q^{(r)}\right) \quad (18),$$

that is found to exhibit exactly a single main lobe around the true angle $\bar{\alpha}_q$ associated to $\bar{\tau}_q$. $\bar{g}_{\bar{\tau}}(\tau)$ was used with lemma 1 to generate required delay realizations $\{\tau_q^{(r)}\}_{r=1}^{R}$ ~ $\bar{g}_{\bar{\tau}}(\tau)$ for every q=1,2,3….., $\bar{Q}$ as follows:

lemma1: let x ∈ X be any RV with pdf $f_X(x)$ and CDF $F_X(x)$ and denote the inverse CDF $F_X^{-1}(.)$: [0, 1] →X, u→X such that $F_X(x) = u$, Then, for any uniform RV, $\tilde{X} = F_x^{-1}(U)$ is distributed according to $f_x(.)$.

1- Generate R realizations $\{u_q^{(r)}\}_{r=1}^{R}$ ~ U[0,1],

2- Obtain $\tau_q^{(r)} = \bar{G}_{\bar{\tau}}^{-1}\left(u_q^{(r)}\right)$ where $\bar{G}_{\bar{\tau}}(.)$ is the cumulative distribution function associated to $\bar{g}_{\bar{\tau}}(\tau)$.

The two steps were performed because depending on the SNR, the direct use of the marginal pdf $\bar{g}_{\bar{\tau}}(\tau)$ faces the following major problems in practice:

1- At low SNR, outliers $\tau = \bar{G}_{\bar{\tau}}^{-1}(u)$, which are delay realizations that don't correspond to any of the true delays, would appear from realization, u ~ U[0,1]that falls within the range of spurious slopes (along the y−axis) in the CDF $\bar{G}_{\bar{\tau}}(\tau)$, as seen in Fig. 2(a),

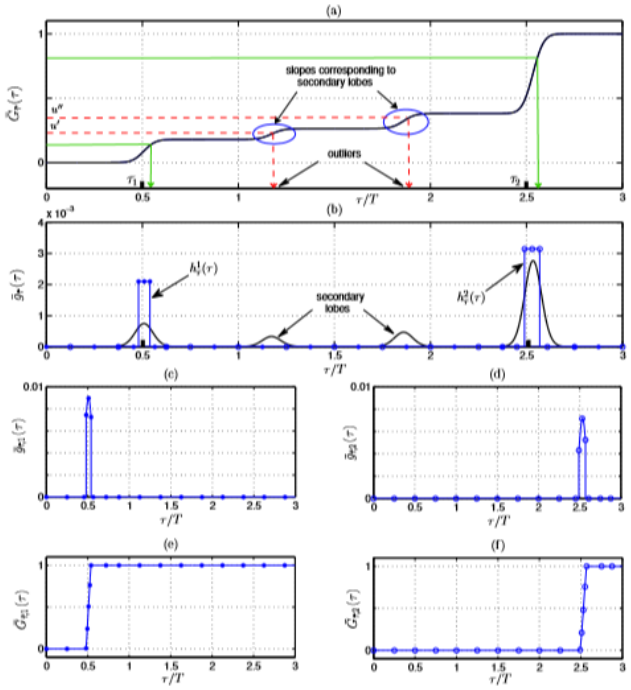

Figure 2. Pseudo-pdfs in a single-carrier system illustrated for $\bar{Q}$ = 2 and SNR = −5 dB: (a) marginal CDF of τ, (b) marginal pdf of τ, (c) local pdf of τ around $\bar{\tau}_1$, (d) local pdf of τ around $\bar{\tau}_2$, (e) local CDF of τ around $\bar{\tau}_1$, and (f) local CDF of τ around $\bar{\tau}_2$.

And which are coming from secondary slopes that are exhibited from $\bar{g}_{\bar{\tau}}(\tau)$, as shown in fig. 2(b)

This phenomenon is also illustrated in Fig. 2(a) for the two typical realizations u' and u''. In order to obtain outliers-free realizations, we could rid $\bar{g}_{\bar{\tau}}(\tau)$ from its secondary lobes by choosing a sufficiently large value for the design parameter ρ1. But taking a large value for ρ1, however, renders the main lobes in $\bar{g}_{\bar{\tau}}(\tau)$extremely narrow making it more likely that the true delays lie outside their very short spans. And so, all outliers-free realizations will be shifted, resulting in an inevitable estimation bias.

2-At sufficiently high SNR levels, the secondary lobes are naturally absent and thus a small value for ρ1 can be chosen. Since the difference in main lobes' sizes results in out-of-proportion slopes in the CDF, an unbalanced number of realizations will be generated under the different main lobes. As a brute-force remedy, one could be tempted by choosing an

extremely large value of realizations to guarantee that a sufficient number of realizations be generated under each main lobe. In order to solve all these problems, we have to use a method that allows to generate all the realizations around the true delays and angles, and ensure that the realizations are generated in exactly the same number under each of the main lobes irrespectively of their relative sizes.

To do so, initial estimates of the unknown true TDs, are extracted through broad line search in equation (53) in [9] as follows:

$$[\hat{\bar{\tau}}_1^{(0)}, \hat{\bar{\tau}}_2^{(0)}, ..., \bar{\tau}_{\bar{Q}}^{(0)}] = \arg\max_{\tau}{}_{\bar{Q}}\ \bar{\vartheta}_{\bar{\tau}}(\tau) \quad (18)$$

Where $\arg\max_{\bar{Q}}\{.\}$ returns the positions of the $\bar{Q}$ largest peaks of any objective function. This initial broad line search is performed using a relatively large grid step $\Delta_{\bar{\tau}}$, and it doesn't provide the delay MLEs even by taking an arbitrarily small value for $\Delta_{\bar{\tau}}$, because the main lobes of $\bar{g}_{\bar{\tau}}(\tau)$ are shifted as in figure(3):

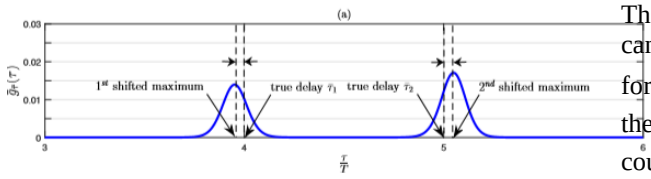

Figure3. main lobes shifting

And initial estimates for the associated AoAs are obtained as in equation (54) in [9] as:

$$\hat{\bar{\alpha}}_q^{(0)} = \arg\max_{\alpha}\ \bar{\vartheta}_{\bar{\alpha}/\bar{\tau}}\left(\alpha \middle/ \tau = \hat{\bar{\tau}}_q^{(0)}\right),\ q = 1, \ldots,\ \bar{Q} \quad (19)$$

That is performed also with a large grid step. So to force $\{\tau_q^{(r)}\}_{r=1}^{R}$ and $\{\alpha_q^{(r)}\}_{r=1}^{R}$ to be generated in the vicinity of $\bar{\tau}_q$ and $\bar{\alpha}_q$, respectively, the following $\bar{Q}$ local intervals were fixed as in [9] as follows:

$$D_{\hat{\bar{\tau}}_q^{(0)}} = \left[\hat{\bar{\tau}}_q^{(0)} - \delta_{\bar{\tau}}, \hat{\bar{\tau}}_q^{(0)} + \delta_{\bar{\tau}}\right]$$

And

$$D_{\hat{\bar{\alpha}}_q^{(0)}} = \left[\hat{\bar{\alpha}}_q^{(0)} - \delta_{\bar{\alpha}}, \hat{\bar{\alpha}}_q^{(0)} + \delta_{\bar{\alpha}}\right]$$

Which are centered at $\hat{\bar{\tau}}_q^{(0)}$ and $\hat{\bar{\alpha}}_q^{(0)}$. And the sizes of local delay and angle intervals are governed by the design parameters $\delta_{\bar{\tau}}$ and $\delta_{\bar{\alpha}}$, and the associated delay and angle impulse functions were defined as follows:

$$h_{\hat{\bar{\tau}}_q^{(0)}}(\tau) = \begin{cases} h_{\bar{\tau}}^q, \ for \tau \in D_{\hat{\bar{\tau}}_q^{(0)}} \\ 0, otherwise \end{cases} \quad (20)$$

$$h_{\hat{\bar{\alpha}}_q^{(0)}}(\alpha) = \begin{cases} h_{\bar{\alpha}}^q, \ for \alpha \in D_{\hat{\bar{\alpha}}_q^{(0)}} \\ 0, otherwise \end{cases} \quad (21)$$

Then the q^{th} delay and angle pseudo-pdfs which are referred to hereafter as local pseudo-pdfs will be used to generate the realizations in $D_{\hat{\bar{\tau}}_q^{(0)}}$ and $D_{\hat{\bar{\alpha}}_q^{(0)}}$ are given by equations (57) and (58) in [9]:

$$\bar{g}_{\bar{\tau},q}(\tau) = h_{\bar{\tau}}^q(\tau)\,\bar{g}_{\bar{\tau}}(\tau) \quad (22)$$

$$\bar{g}_{\bar{\alpha}/\bar{\tau},q}(\alpha/\tau) = h_{\bar{\tau}}^q(\alpha)\,\bar{g}_{\bar{\alpha}/\bar{\tau}}(\alpha/\tau) \quad (23)$$

For $q = 1,2,...\bar{Q}$, the constants $h_{\bar{\tau}}^q$ and $h_{\bar{\alpha}}^q$, are computed such that the local pseudo-pdfs in (22) and (23) sum up to one thereby yielding equations (59) and (60) in [9] as follows:

$$h_{\bar{\tau}}^q = \left(\int_{\hat{\bar{\tau}}_q^{(0)} - \delta_{\tau}}^{\hat{\bar{\tau}}_q^{(0)} + \delta_{\tau}} \bar{\vartheta}_{\bar{\tau}}(\tau) dt \right)^{-1} \quad (24)$$

$$h_{\bar{\alpha}}^q = \left(\int_{\hat{\bar{\alpha}}_q^{(0)} - \delta_{\alpha}}^{\hat{\bar{\alpha}}_q^{(0)} + \delta_{\alpha}} \bar{\vartheta}_{\bar{\alpha}/\bar{\tau}}(\alpha/\tau) d\alpha \right)^{-1} \quad (25)$$

Then by applying the impulse functions in (22) and (23), we can obtain a separate isolated local angle/delay pseudo-pdf for each q^{th} path. So, in practice, the processes of generating the required realizations locally around each true delay/angle couple, $(\bar{\alpha}_q, \bar{\tau}_q)$, can be implemented separately and run in parallel with faster and less complex execution. For better illustration, figures 2(c) and 2(d) show the isolated local delay pseudo-pdfs, $\bar{\vartheta}_{\bar{\tau},1}(\tau)$ and $\bar{\vartheta}_{\bar{\tau},2}(\tau)$, in case of $\bar{Q} = 2$. And as seen from figures 2-e and 2-f, the associated local CDFs, $\bar{G}_{\bar{\tau},1}(\tau)$ and $\bar{G}_{\bar{\tau},2}(\tau)$, exhibit a single slope that is located around the corresponding true delay. So by applying the result of lemma 1, each uniform realization $u_q^{(r)} \in [0,1]$ will yield a delay realization $\tau_q^{(r)} \in D_{\hat{\bar{\tau}}_q^{(0)}}$ in the vicinity of $\bar{\tau}_q$. And so all angle realizations that are generated using the q^{th} isolated conditional pdfs fall in the vicinity of $\bar{\alpha}_q$.

Then we can apply implementation details in section 8 in [9], on equation (6) in this paper, to localize the adversary.

These implementation details are:

1-Local generation of the required realizations:

Step1:

Evaluate the joint pdf $\bar{\vartheta}_{\bar{\alpha},\bar{\tau}}(\alpha,\tau)$ locally at new discrete points $\alpha_i', \tau_j' \in D_{\hat{\bar{\alpha}}_q^{(0)}} \times D_{\hat{\bar{\tau}}_q^{(0)}}$ as in equation (61) in [9] which is:

$$\bar{\vartheta}_{\bar{\alpha},\bar{\tau}}(\alpha_i,\tau_j) = \frac{\exp\{p1I(\alpha_i,\tau_j)\}}{\sum_i \sum_j \exp\{p1I(\alpha_i,\tau_j)\}\Delta_{\bar{\tau}}^{broad}\Delta_{\bar{\alpha}}^{broad}} \quad (26),$$

which is the evaluation of the periodogram $I(\alpha_i,\tau_j)$ at multiple grid points (α_i,τ_j) with large discretization steps $\Delta_{\bar{\alpha}}^{broad}$ and $\Delta_{\bar{\tau}}^{broad}$, and then approximating integrals with discrete sums to evaluate the joint pdf

Step2: compute the q^{th} marginal delay pdf at every point $\tau_j' \in D_{\hat{\bar{\tau}}_q^{(0)}}$ as in equation (62) in [9] which is:

$$\bar{\vartheta}_{\bar{\tau}}(\tau_j) = \sum_i \bar{\vartheta}(\alpha_i,\tau_j)\Delta_{\bar{\alpha}}^{broad},\ \forall \tau_j \in [0,\tau_{\max}]$$

Where the initial delay estimates $\left\{\hat{\bar{\tau}}_q^{(0)}\right\}_{q=1}^{\bar{Q}}$ are the discrete delay points that correspond to the largest $\bar{Q}$ maxima of (27), then for each q=1, 2… $\bar{Q}$, the conditional pdf of the q^{th} angle corresponding to $\hat{\bar{\tau}}_q^{(0)}$, can be obtained as in equation (63) in [9] as:

$$\bar{\vartheta}_{\bar{\alpha}/\bar{\tau}}\left(\alpha_i \middle/ \tau=\hat{\bar{\tau}}_q^{(0)}\right)=\frac{\bar{\vartheta}_{\bar{\alpha},\bar{\tau}}\left(\alpha_i,\hat{\bar{\tau}}_q^{(0)}\right)}{\bar{\vartheta}_{\bar{\tau}}\left(\hat{\bar{\tau}}_q^{(0)}\right)},\forall\alpha_i\in\left[-\frac{\Pi}{2},\frac{\Pi}{2}\right] \quad (27)$$

Then we could have equation (64) in [9] as:

$$\bar{\vartheta}_{\bar{\tau},q}\left(\tau_j'\right)=\sum\bar{\vartheta}\left(\alpha_i',\tau_j'\right)\Delta_{\bar{\alpha}}^{small}\quad\forall\tau_j'\in D_{\hat{\bar{\tau}}_q^{(0)}} \quad (28)$$

Step 3:

Compute the q^{th} local delay CDF as equation (65) in [9] as follows:

$$\bar{G}_{\bar{\tau},q}(\tau_j')=\sum_{l\le j}\bar{\vartheta}_{\bar{\tau},q}(\tau_l')\Delta_{\bar{\tau}}^{small}\quad\forall\tau_j'\in D_{\hat{\bar{\tau}}_q^{(0)}} \quad (29)$$

Step 4:

Generate R realizations $\left\{u_q^{(r)}\right\}_{r=1}^{R}\sim U[0,1]$ and invert $\bar{G}_{\bar{\tau},q}(.)$ via linear interpolation in order to obtain the local delay realizations $\tau_q^{(r)}=\bar{G}_{\tau,q}^{-1}\left(u_q^{(r)}\right)$ for r=1, 2…R.

Step 5:

For r=1, 2… R, obtain immediately the local pdf of the q^{th} AOA conditioned on $\tau_q^{(r)}$ from the local joint pdf that are evaluated in step1 as equation (65) in [9] as follows:

$$\bar{\vartheta}_{\bar{\alpha}/\bar{\tau}}\left(\alpha_i' \middle/ \tau=\tau_q^{(r)}\right)=\frac{\bar{\vartheta}_{\bar{\alpha},\bar{\tau}}\left(\alpha_i',\tau_q^{(r)}\right)}{\bar{\vartheta}_{\bar{\tau},q}\left(\tau_q^{(r)}\right)}\quad\forall\alpha_i'\in D_{\hat{\bar{\alpha}}_q^{(0)}} \quad (30)$$

Step 6:

Evaluate the q^{th} local angle CDF, $\bar{G}_{\bar{\alpha},q}\left(\alpha_i'\right)$ similarly to, $\bar{G}_{\bar{\tau},q}\left(\tau_j'\right)$, in (29), and generate the r^{th} angle realization $\alpha_q^{(r)}=\bar{G}_{\bar{\alpha},q}^{-1}\left(u_q^{(r)}\right)$, using linear interpolation also.

2-Estimation of time delays and angle of arrivals

After generation of all the required realizations, more accurate IS-based parameter estimates can were obtained by applying the circular sample mean instead of the linear sample mean. Because the latter averages out all the realizations and outlier seeds will result in an inevitable estimation bias. However, the circular mean succeeds in selecting the best angle and delay realizations in terms of Euclidean distance to the true multipath-resolution parameters. The circular mean of any transformation $f(\Phi)$ of a given random variable $\Phi\in[-\pi,\pi]$ with distribution $p_\phi(\phi)$ is obtained as equation (66) in [9] as follows:

$$\hat{\bar{\phi}}=\angle\frac{1}{R}\sum_{r=1}^{R}f(\phi^{(r)})e^{j\phi^{(r)}} \quad (31)$$

Where, where φ(r) ~ pΦ(.) are R realizations of Φ.

We need to transform $\tau_q^{(r)}$ and $\alpha_q^{(r)}$ that are respectively in $[0,\tau_{\max}]$ and $[-\pi/2,\pi/2]$ into interval $[-\pi,\pi]$.So transformations

$\Phi_1(\tau_q^{(r)})=2\pi(\tau_q^{(r)}/\tau_{\max}-1/2)\in[-\pi,\pi]$ and

$\Phi_2(\alpha_q^{(r)})=2\alpha_q^{(r)}\in[-\pi,\pi]$, were applied for Uniform Linear Arrays (ULAs).so the circular mean is first applied using $\Phi_1(\tau_q^{(r)})$ and $\Phi_2(\alpha_q^{(r)})$, then the true TDs and AoAs are then estimated using the inverse transformations

$\Phi_1^{-1}(x)=\tau_{\max}(\frac{1}{2}+\frac{1}{2\pi}x)$ and $\Phi_2^{-1}(x)=\frac{1}{2}x$ as as in equations (67) and (68) in [9] as follows:

$$\hat{\bar{\tau}}_q=\tau_{\max}\left(\frac{1}{2\pi}<\left[\sum_{r=1}^{R}\eta\left(\alpha^{(r)},\tau^{(r)}\right)e^{j2\pi\left(\frac{\tau_q^{(r)}}{\tau_{\max}}-\frac{1}{2}\right)}\right]+\frac{1}{2}\right) \quad (32)$$

$$\hat{\bar{\alpha}}_q=\frac{1}{2}<\left[\sum_{r=1}^{R}\eta\left(\alpha^{(r)},\tau^{(r)}\right)e^{j\left(2\alpha_q^{(r)}-\pi\right)}\right] \quad (33)$$

Where the weighting coefficient was expressed as equation (69) as:

$$\eta(\alpha^{(r)},\tau^{(r)})=\frac{\mu\exp\{P_0\varsigma_c(\alpha^{(r)},\tau^{(r)})\}}{\exp\{P_1\sum_{q=1}^{\bar{Q}}I(\alpha_q^{(r)},\tau_q^{(r)})\}} \quad (34)$$

where

$$\mu=\frac{\int\ldots\int\exp\{P_1\sum_{q=1}^{\bar{Q}}I(\alpha_q,\tau_q)\}d\alpha d\tau}{\int\ldots\int\exp\{P_0\varsigma_c(\alpha,\tau)\}d\alpha d\tau} \quad (35)$$

By defining the quantity:

$$\Psi(\alpha,\tau)\triangleq P_0\varsigma_c(\alpha,\tau)-P_1\sum_{q=1}^{\bar{Q}}I(\alpha_q,\tau_q) \quad (36)$$

And using the following normalized weighting coefficient

$\bar{\eta}(\alpha^{(r)},\tau^{(r)})=\exp\{\Psi(\alpha^{(r)},\tau^{(r)})-\max_{1\le r\le R}\Psi(\alpha^{(r)},\tau^{(r)})\}$ (37)

instead of the weighting coefficient $\eta(\alpha^{(r)},\tau^{(r)})$ in (34)

To reduce the computational load with no changes in the final results.

To generate vector realizations that jointly minimize the Euclidean distance to the true delay and angle parameters, such that:

$$[\hat{\bar{\tau}},\hat{\bar{\alpha}}]=\arg\min_{\tau^{(r)},\alpha^{(r)}}(\left\|\tau^{(r)}-\bar{\tau}\right\|^2+\left\|\alpha^{(r)}-\bar{\alpha}\right\|^2) \quad (38)$$

This is according to lemma 2 which says that:

The circular-mean estimates $\hat{\bar{\tau}}=[\hat{\bar{\tau}}_1,\hat{\bar{\tau}}_2,\ldots,\hat{\bar{\tau}}_{\bar{Q}}]$ and $\hat{\bar{\alpha}}=[\hat{\bar{\alpha}}_1,\hat{\bar{\alpha}}_2,\ldots,\hat{\bar{\alpha}}_{\bar{Q}}]$, obtained in (32) and (33) by using the normalized factor in (37) correspond to the vector realizations that jointly minimize

the Euclidean distance to the true delay and angle parameters. These circular-mean estimates are applied to obtain more accurate IS-based parameter estimates, other than linear sample mean estimates, as shown before.

Where the weighting coefficient was expressed as equation (69) as:

$$\eta(\alpha^{(r)},\tau^{(r)})=\frac{\mu\exp\{P_0\varsigma_c(\alpha^{(r)},\tau^{(r)})\}}{\exp\{P_1\sum_{q=1}^{\bar{Q}}I(\alpha_q^{(r)},\tau_q^{(r)})\}} \quad (39)$$

And

$$\mu=\frac{\int...\int\exp\{P_1\sum_{q=1}^{\bar{Q}}I(\alpha_q,\tau_q)\}d\alpha d\tau}{\int...\int\exp\{P_0\varsigma_c(\alpha,\tau)\}d\alpha d\tau} \quad (40)$$

And defining the quantity:

$$\Psi(\alpha,\tau)\ \underline{\underline{\Delta}}P_0\varsigma_c(\alpha,\tau)-P_1\sum_{q=1}^{\bar{Q}}I(\alpha_q,\tau_q) \quad (41)$$

To generate vector realizations that jointly minimize the Euclidean distance to the true delay and angle parameters, such that:

$$[\hat{\bar{\tau}},\hat{\bar{\alpha}}]=\arg\min_{\tau^{(r)},\alpha^{(r)}}(\left\|\tau^{(r)}-\bar{\tau}\right\|^2+\left\|\alpha^{(r)}-\bar{\alpha}\right\|^2) \quad (42)$$

Stage 1:

Generate R1 << R2, $\{\tau_q^{(r)}\}_{r=1}^{R1}$ and $\{\alpha_q^{(r)}\}_{r=1}^{R1}$ in the local intervals $D_{\hat{\bar{\tau}}_q^{(0)}}$ and $D_{\hat{\bar{\alpha}}_q^{(0)}}$, and obtain the estimates $\hat{\bar{\tau}}_q$ and $\hat{\bar{\alpha}}_q$ as in (32) and (33).

It was found that initial estimates $\hat{\bar{\tau}}_q^{(0)}$ and $\hat{\bar{\alpha}}_q^{(0)}$ are shifted respectively by at most $\in_\tau$ and $\in_\alpha$ from the true delays and angles such that $\left|\hat{\bar{\tau}}_q^{(0)}-\bar{\tau}_q\right|\le\in_\tau$ and $\left|\hat{\bar{\tau}}_q^{(0)}-\bar{\tau}_q\right|\le\in_\alpha$. And the exact MLEs are obtained by IS-based estimates in (32) and (33), with R0 = 20000 realizations that are generated locally using $\delta_{\bar{\tau}}=2\in_\tau$ and $\delta_{\bar{\alpha}}=2\in_\alpha$, and using normalized weighting coefficients as in equation (72) in [9] as follows:

$$\bar{\eta}(\alpha^{(r)},\tau^{(r)})=\exp\{\Psi(\alpha^{(r)},\tau^{(r)})-\max_{1\le r\le R}\Psi(\alpha^{(r)},\tau^{(r)})\} \quad (43)$$

Note that the typical values for $\delta_{\bar{\tau}}$ and $\delta_{\bar{\alpha}}$ are chosen so that the corresponding local intervals $D_{\hat{\bar{\tau}}_q^{(0)}}=[D_{\hat{\bar{\tau}}_q^{(0)}}-\delta_{\bar{\tau}},D_{\hat{\bar{\tau}}_q^{(0)}}+\delta_{\bar{\tau}}]$ and $D_{\hat{\bar{\alpha}}_q^{(0)}}=[D_{\hat{\bar{\alpha}}_q^{(0)}}-\delta_{\bar{\alpha}},D_{\hat{\bar{\alpha}}_q^{(0)}}+\delta_{\bar{\alpha}}]$ include the true values of the unknown parameters because they verify $\left|\hat{\bar{\tau}}_q^{(0)}-\bar{\tau}_q\right|\le\delta_{\bar{\tau}}/2$ and $\left|\hat{\bar{\alpha}}_q^{(0)}-\bar{\alpha}_q\right|\le\delta_{\bar{\alpha}}/2$. And this ensures that a portion of the R0 = 20000 realizations are generated on both sides of each true TD and AoA.

Stage 2:

Regenerate R2 << R0 new realizations $\{\tau_q'^{(r)}\}_{r=1}^{R2}$ and $\{\alpha_q'^{(r)}\}_{r=1}^{R2}$ over narrower intervals that are centered around the estimates $\hat{\bar{\tau}}_q$ and $\hat{\bar{\alpha}}_q$ obtained in stage1, such that $D'_{\hat{\bar{\tau}}_q}=\left[\hat{\bar{\tau}}_q-\delta'_{\bar{\tau}},\hat{\bar{\tau}}_q+\delta'_{\bar{\tau}}\right]$ and $D'_{\hat{\bar{\alpha}}_q}=\left[\hat{\bar{\alpha}}_q-\delta'_{\bar{\alpha}},\hat{\bar{\alpha}}_q+\delta'_{\bar{\alpha}}\right]$ with $\delta'_{\bar{\tau}}=\delta_{\bar{\tau}}/10$ and $\delta'_{\bar{\alpha}}=\delta_{\bar{\alpha}}/10$, then compute the AOA Maximum Likelihood estimation (MLE), using the new angle realizations, $\left\{\alpha'^{(r)}=\left[\alpha_1'^{(r)},\alpha_2'^{(r)},...,\alpha_{\bar{Q}}'^{(r)}\right]\right\}_{r=1}^{R2}$ and the delay estimates $\hat{\bar{\tau}}=\left[\hat{\bar{\tau}}_1,\hat{\bar{\tau}}_2,...,\hat{\bar{\tau}}_{\bar{Q}}\right]^{\mathrm{T}}$ obtained in stage 1 as equation (74) in [9] as follows:

$$\hat{\bar{\alpha}}_{q,MLE}=\frac{1}{2}<\left[\sum_{r=1}^{R2}\bar{\eta}\left(\alpha'^{(r)},\hat{\bar{\tau}}\right)e^{j\left(2\alpha_q'^{(r)}-\pi\right)}\right] \quad (44)$$

Then all the AOA MLEs obtained in (43), $\hat{\bar{\alpha}}_{MLE}=\left[\hat{\bar{\alpha}}_{1,MLE},\hat{\bar{\alpha}}_{2,MLE},...,\hat{\bar{\alpha}}_{\bar{Q},MLE}\right]^{\mathrm{T}}$, are then used with the delay realizations, $\left\{\tau'^{(r)}=\left[\tau_1'^{(r)},\tau_2'^{(r)},...,\tau_{\bar{Q}}'^{(r)}\right]\right\}_{r=1}^{R2}$ to find the Time Delay (TD MLEs) as equation (75) in [9] as follows:

$$\hat{\bar{\tau}}_{q,MLE}=\tau_{\max}\left(\frac{1}{2\Pi}<\sum_{r=1}^{R2}\bar{\eta}\left(\tau'^{(r)},\hat{\bar{\alpha}}_{MLE}\right)e^{j2\pi\left(\frac{\tau_q'^{(r)}}{\tau_{\max}}-\frac{1}{2}\right)}+\frac{1}{2}\right) \quad (45)$$

So, the MLEs obtained in (43) and (44) are not constrained to be on the considered sampling grid (the PDF of the time-varying scattering coefficient in equation (6), because the generated angle and delay realizations are not constrained to be on the grid points due to the use of the linear interpolation in STEP 4 and STEP 6 in "Local Generation of the Required Realizations" section

Then when assessing the performance of importance sampling-based maximum likelihood (IS-based ML) estimator in terms of root mean square error (RMSE) which determined for each q^{th} time delay and angle of arrival.

$$\text{RMSE}=\sqrt{\frac{\sum_{m=1}^{Mc}\left(\hat{\bar{\tau}}_{q,MLE}^{[m]}-\bar{\tau}_q\right)^2}{Mc}} \quad (46)$$

$$\text{RMSE (deg)}=\sqrt{\frac{\sum_{m=1}^{Mc}\left(\hat{\bar{\tau}}_{q,MLE}^{[m]}-\bar{\alpha}_q\right)^2}{Mc}} \quad (47)$$

Where Mc = 5000 is the total number of Monte-Carlo runs, in all simulations, and $\hat{\bar{\tau}}_{q,MLE}^{[m]}$ and $\hat{\bar{\alpha}}_{q.MLE}^{[m]}$ are, respectively, the estimates of $\bar{\tau}_q$ and $\bar{\alpha}_q$ during the m^{th} Monte-Carlo run.

And then obtaining the joint ML estimates of $\bar{\alpha}$ and $\bar{\tau}$ as a solution to reduced – dimension optimization problem in equation (6) [9].

$$\left[\bar{\alpha}_{\mathrm{MLE}},\bar{\tau}_{\mathrm{MLE}}\right]=\arg\max_{\alpha,\tau}\varsigma_{\mathrm{c}}(\alpha,\tau) \quad (48)$$

In order to find the maximum likelihood estimates for all unknown path gains, $\hat{\bar{\gamma}}_{MLE}$. An important aspect of the proposed detection system is that this system can differentiate two devices even at the same location, which was not well addressed by previous approaches. Our extensive experimental results demonstrated the effectiveness of the system, even when devices are co-located. In [20] they showed how directionality and gain at the physical layer affects the received power. And we used this idea to detect and localize the adversary especially in adaptive beam forming [21] where a direction of arrival (DOA) algorithm can be used to determine the direction of the signal received from the user. In [9], they depended on estimating number of paths of the received signal, but we depended on determining paths of the received signal in the reproduced statistical location of scatterers, to make the detection and localization more accurate, increase the performance of the localization algorithm. In [9], they depended on the Expectation of $\mathrm{P}(Q)$, (i.e.: $E\{\mathrm{P}(Q)\}$) to determine the number of signal paths, such that:

$$\mathrm{P}(Q)=\frac{\sum_{q}^{Q}\left|\bar{g}_{\bar{\mathrm{T}}}\left(\dot{\mathrm{T}}_{q}\right)\right|^{2}}{\sum_{q}^{Q_{tot}}\left|\bar{g}_{\bar{\mathrm{T}}}\left(\dot{\mathrm{T}}_{q}\right)\right|^{2}}\geq \mathrm{K} \quad (49)$$

And

$$\mathrm{P}(Q-1)=\frac{\sum_{q}^{Q-1}\left|\bar{g}_{\bar{\mathrm{T}}}\left(\dot{\mathrm{T}}_{q}\right)\right|^{2}}{\sum_{q}^{Q_{tot}}\left|\bar{g}_{\bar{\mathrm{T}}}\left(\dot{\mathrm{T}}_{q}\right)\right|^{2}}<\mathrm{K} \quad (50)$$

, and they made these two simple steps to get the number of signal paths where they depended to optimize the threshold level, K, offline, in [9], to obtain lowest $\overline{Q}$ estimation error. They made Monte-Carlo simulations for all $1\leq Q\leq Q_{tot.}$, and these two simple steps which are:

1-getting the points $\left\{\dot{\mathrm{T}}_{q}\right\}_{q}^{Q_{tot.}}$, corresponding to all peaks in $\{\bar{\mathrm{g}}_{\mathrm{T}}(\mathrm{T_i})\forall\,\mathrm{T_i}\in[0,\mathrm{T_{max}}]\}$ with $\mathrm{Q_{tot}}$ being total number of peaks where $\mathrm{Q_{tot}}$ is always greater than $\overline{Q}$ due to the presence of secondary lobes

2- Sorting the squared magnitudes $\left\{\left|\bar{g}_{\bar{\mathrm{T}}}\left(\dot{\mathrm{T}}_{q}\right)\right|^{2}\right\}_{q}^{Q_{tot.}}$, corresponding to $\left\{\dot{\mathrm{T}}_{q}\right\}_{q}^{Q_{tot.}}$ to get an estimate $\hat{\overline{Q}}$ for the actual number of paths as the first number of peaks Q whose combined energy frictions is above the threshold K

2- Designing the data sample to be representative, and spatially balanced (well-spread). As discussed in above. The sample is said to be representative sample if each coherent subset has the same proportion of the population and it is said to be spatially balanced if for each coherent subset, the number of sampled units is approximately equal to the summation of inclusion probability for each element in the coherent subset, so the sample design we made was with equal inclusion probability, such that all population units was included in the sample with equal probability, so we generated a well spread sample, and so it was representative.

5. Results

We showed how to use angle of arrival of scatterers [4, 5] in detection and localization of adversaries in homogeneous wireless networks. The observation of the pattern of received signal and its identification was based on the observation of the signal strength (intensity), and its direction. This is a spatial behavior in space, and it characterizes the spatial relationship between selected points in the space of surrounding scattered areas.

5.1 Sampling that verified the Geometrical Channel Model (GCM)

We showed above, that collection sampling we incorporated, has improved coherence and it was accurate sampling that can capture the needed characteristics in the geometry of receiver's surrounded area (scatterers) [5], to detect the anomaly, and localize its source, by means of points in pointing vectors, through beam width of angle of arrival [9]. And this would be deterministic due to the predefined sampled points in the incorporated geometry of scatterers structure instead of a predicted modeled spatial structure [10].

In [18], they defined the coherent subset as follows:

Let $\mathrm{i}\in\mathrm{u}$ and let $\mathrm{r}\geq 0$ be a given radius. We say that U^{*}, is a coherent subset of U if the following holds. Unit $j\in U$ is included in U^{*} if and only if $\mathrm{d}(i,j)\leq r$, where $\mathrm{d}(i,j)$ is the distance between i and j, thus U^{*}, can be constructed by including all units within a ball of radius r from some unit i.

So, a coherent subset U^{*}, of a population, can be formed from j units if distance between j and i less than or equal to a specified radius, where i element in U.

The number of sampled units n^{*} from the coherent subset U^{*} can be expressed by:

$n^{*}=(n/N)N^{*}$, where n is the sample size, and N is the number of units of population, and N^{*} is the size of U^{*}

.5.2 in our simulation, all spoofed frames were detected

In our simulation, all spoofed frames were detected, and neither false positive nor false negative alarm was raised. As showed in [22], the effect of a parabolic reflector on Wi-Fi reception was discussed and when analyzing results in [22] and analyzing results in [5] and [9], we found that in [22], the power distribution on direct path component and components of local scattering is showed from the Focal point where the signal powers were the best at all three fitting positions of the Focal, Inner (= 1/2 focal length), and Outer (= 3/2 focal length) points. and in [5], when using the scattered transfer function to observe the amplitude in figure 4, it was observed that as travel distance increase, as power of single bounced rays and double bounced rays decrease but power slightly rises with the increase of travel distance, this is because increasing travel distance leads to increasing in incidence angle in the their geometry, and reflection loss rapidly decrease as figure 5 shows, faster than growth rate of distance-dependent loss. And this results in increase tendency which proves significance of angle information in modeled transfer function. Note that ray power with travel

distance and incidence angle, but they used travel distance at the horizontal axis for compaction. And our approach considers the non-stationary as well as the spatial consistency. And in [5] and [22], they used the concept of radius to define the local scattering area but we depended on geometry based stochastic channel model [5] that builds on specific transmitter Tx , receiver Rx and scatterer geometries (scattered ray geometry) that is predefined according to certain statistical distribution of significant scatterers, to define local scattering area to measure the actual angle of arrival and not estimation of it and so we could determine the beam width of a specified received signal. This was shown when we compared our results to the idea of power spatial density in hyperbolic scattering areas [22], and we found that our results are going with results in [22] and [5] and [4] in the distance between the sender and receiver, that influences on the amplitude.

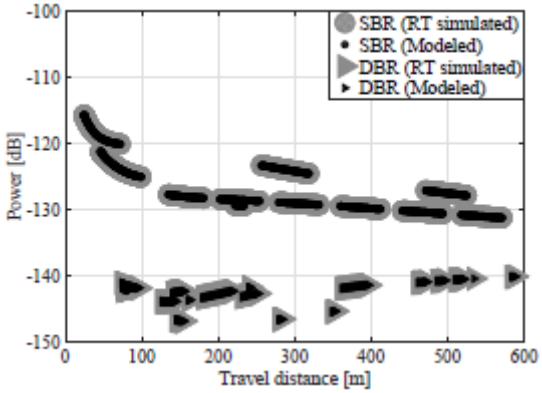

Figure 4. Comparisons of the ray powers obtaining from the RT simulation and the modeled transfer function for the SBRs and DBRs.

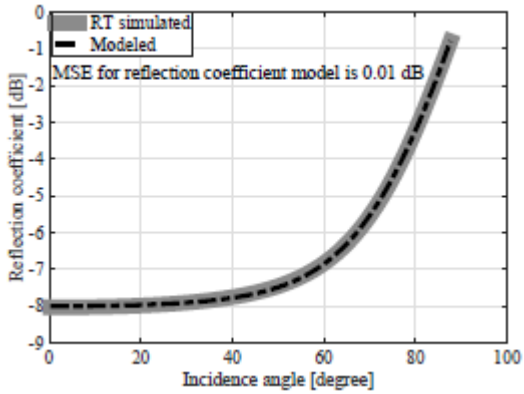

Figure 5. Validation of the model for the reflection coefficients of the SBRs, the reflection coefficient in dB vs. the incidence angle.

Since Probability Distribution Function [4] can be used in finding correlation and decorrelation distances [23], , we selected the sample size as discussed in [18] by assuming that each unit i element in U has a prescribed inclusion probability, so we didn't depend on an estimated surface an in [18], and we depended on analysis of scattered multipath component (SMC), through scattered ray geometry , that gave us the ability to observe the significant scatterer distribution, that are due to flooding of frames at the MAC [24] layer, and it's power observation through the transfere function and scattering coefficients. So this gave us the ability to identify and know the sparsity promoting parameter and measuring the angle of arrival as in [9] with reduced secondary lobes that are caused by the uncertainty of sparsity promoting parameter

According to the difference between what we have proposed and previous researches is that we showed how to enhance the accuracy of detection by depending on real geometry of scatterers, and not estimated surface as in [10]. In our research and experiment we showed the enhancement of the way of detection and localization of multiple adversaries than previous researches, through measurement of angle of arrival and it's beam width, and from the concept of vectors and signal directionality and coherence, instead of previous methods due to co location problem.

6. The Experiment

We have used Optimized Network Engineering Tool (OPNET) in creating a radio dynamic network topology. Figure 6(a) shows the simulation was designed through parametric simulation to show the difference in signal to noise ratio in case of directionality and isotropic wireless radio stationary nodes, through the well spread, and good designed sampling, and the mobile radio wireless node that represents the spoofed node in our simulation experiment. Figure 6(b) shows the locations where the adversary was closest to the receiving node. We have used also the antenna pattern editor to create directional antenna pattern so that we could determine and show the power gain by which the signal was received in the direction of the transmitter of interest.

A legal transmitting wireless node was created to send frames to the wireless receiver node with a uniform strength in all directions without any interference from the adversary. An antenna pattern, with a gain of 50 dB in one direction and a gain of 0 dB in all other directions (directional antenna) was created to use it at the wireless receiver node to see its affect while receiving spoofed frames coming from the adversary node while it was in motion, and see the affect when receiving malicious frames from this adversary with isotropic antenna versus directional antenna.

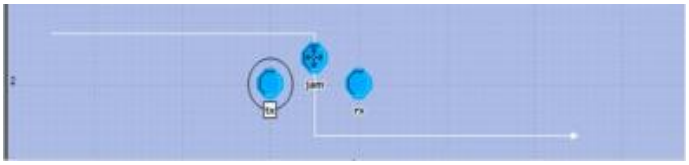

Figure 6 (a) shows the jammer in motion towards closest position relative to the receiver

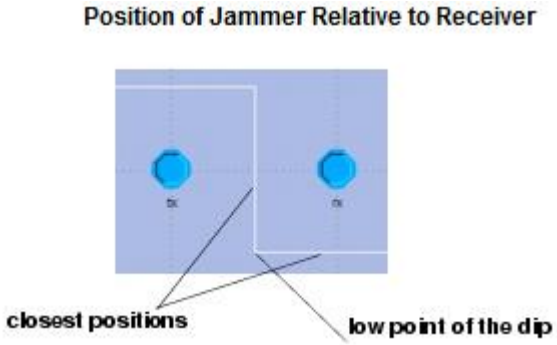

Figure 6 (b) Closest position of jammer relative to receiver

The difference between the attack scenario and the other legal scenario was shown by the adversary node which sends frames that are different in the modulation also, and so appeared to be noise to the receiver and changes the power of legal frames when receiving them.

The scenario also was held while the attacker was in motion towards to and away from the receiver node. And this increased and decreased the interference at receiver. And results of bit error rate, throughput, and received power statistics in case of directional antenna pattern at receiver antenna gain (power coupled statistics) were recorded.

Figure 7(a) records results of the bit error rate, throughput, and received power statistics for the isotropic antenna, with respect to time, and adversary node and transmitter node positions.

Figure 7(b) and figure 7(c) diagrams shows that received power Coupled Statistics of the isotropic gain antenna in receiver. Received power from the transmitter is constant, which is expected since both transmitter and receiver are fixed nodes. The received power from the jamming node follows a similar pattern as the bit error rate in figure 7(a) in that it reached a maximum when the distance between the jamming node and the receiver is smallest. Note that the two humps matched the two locations when the jamming node is closest to the receiver

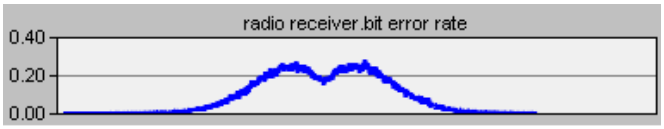

Figure 7(a) shows the bit error rate, At the receiver in presence of jammer

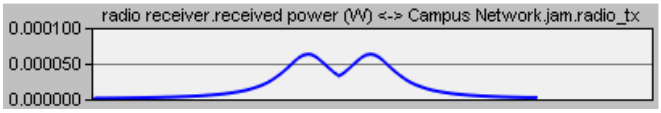

Figure 7(b) shows the received power statistics from the Jammer directional antenna

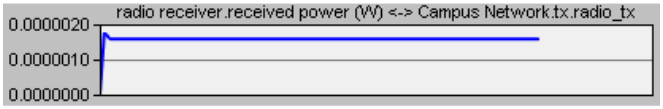

Figure 7(c) shows the received power statistics from the legal stationary isotropic antenna.

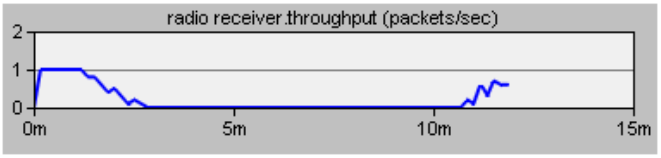

Figure 7(d) shows the statistics of packets received from the stationary transmitter node

Once again from figure 7(a) and 7 (b), the bit error rate pattern matches the received power from the jamming node. The very large power values from transmitter and jamming node are due to the 50dB gain provided by the antenna pattern of the jammer.

The bit error rate at the receiver node is non-zero initially as the distance between the jamming node and receiver node decreases, as in figure 7(a)

However, after about 1 minute, the direction vector between the jamming antenna and the receiver antenna was no longer in line with the direction of greatest gain for the receiver antenna. So, the receiver node stopped receiving interference from the jamming node and the bit error rate at the receiver dropped to 0. This drop dramatically increased the number of packets received (power at figure 7(c)) from the stationary transmitter node (as seen in the graphs 7(a), and 7 (d)

After about 6 minutes, the jamming node comes back into the antenna's cone, at which point the bit error rate increases and the number of packets received first drops (as the jamming node approaches the receiver), then increased again (as the jamming node got far). Once the jamming node leaves the antenna's cone, the bit error rate drops back to 0. When comparing our results to figure 8 [4], we have found that it has the maximum peaks that can be used to get an estimate $\hat{\bar{Q}}$ for actual number of paths.

The following diagram in figure 8 shows the power level peaks with respect to time ,representing variation between the power delay spectrum and it's trend (strength variation between local maximums – the pattern of beam width)).

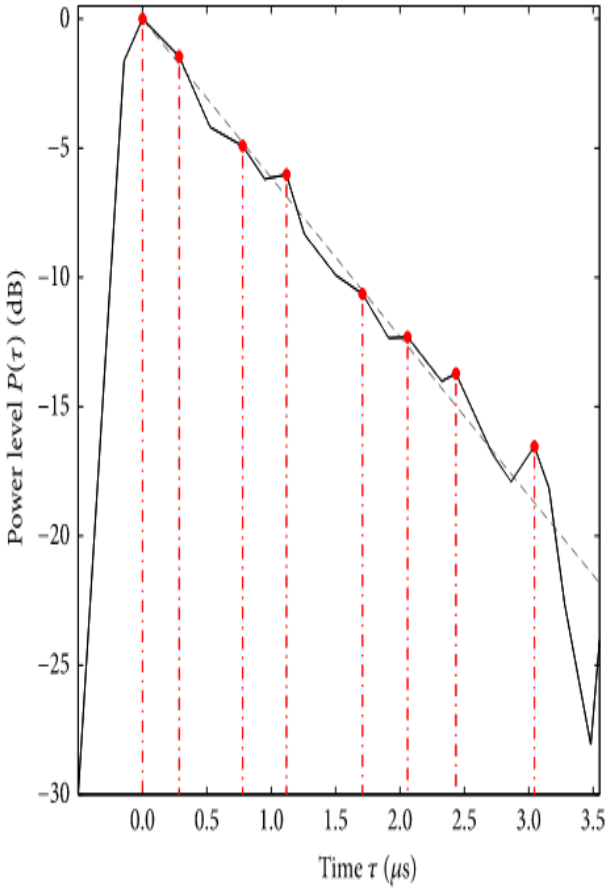

Figure 8. maximum peaks for number of paths

1-In our contribution, we depended on evaluation of the joint pdf in the range angle of scatterers with significant hight power values, because we depended on the periodogram of the signal with only high power values instead of the periodogram of the whole signal (equations 10-12), and assessed the local interval of realizations generation at stage 1 and 2. And so getting angle-delay pairs, and vector realizations $\alpha^{(r)} and \tau^{(r)}$ that can be generated using the multidimensional distribution $\bar{\varsigma}(\alpha,\tau)$ by generating $\bar{Q}$ independent couples (α_q^r, τ_q^r) using $\bar{g}_{\bar{\alpha},\bar{\tau}}(\alpha,\tau)$ that depends on the periodogram of the signal with only high significant power level, and so decreasing the time of evaluation and also errors coming from unwanted secondary lobes and other un significant power. The following diagram in figure 9a shows the periodogram of an ordinary signal and figure 9b shows the periodogram of a jammed signal.

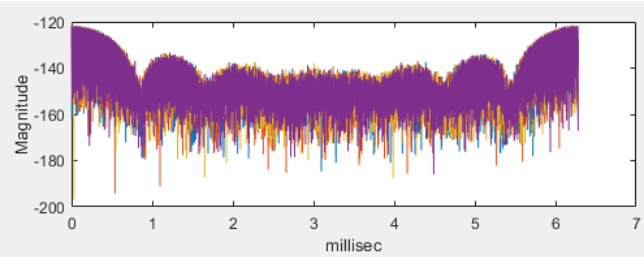

Figure 9a. periodogram of ordinary signal

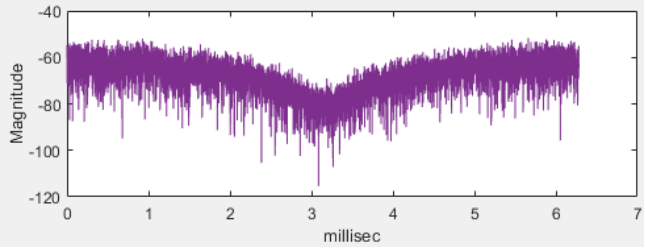

Figure 9b. periodogram of a jammed signal

In stage 2 at equation (39) and (40), we depended on getting the candidate angles within a defined range angle that has only scatterrers with highest power level instead of the whole range angle defined in [9] as [−π/2,π/2] for Uniform Linear Arrays (ULAs), and [0,2π] for Uniform Circular Arrays (UCAs). The following diagram in figure 10 shows the range angle of two signals. One signal originates from 30 degrees azimuth and has a power of 10 W. A second incoming signal originates from 60 degrees azimuth and has a power of 5 W. The two signals are not correlated with each other, and the noise is white across all array elements, and the SNR is 10 dB.

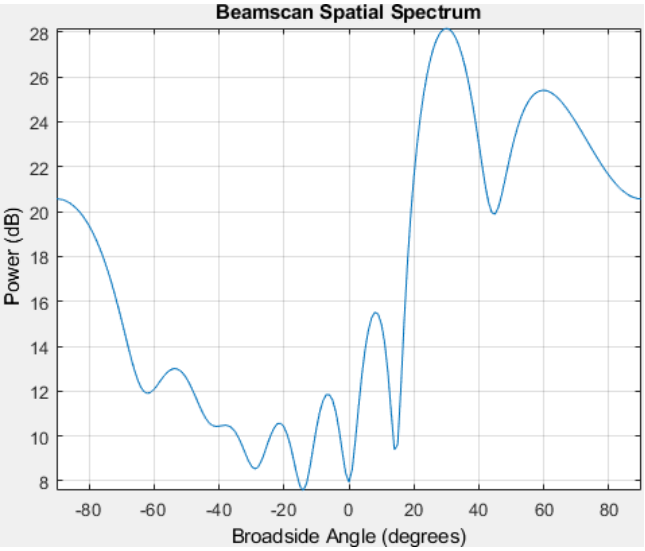

Figure 10: two signals that are not correlated to each other

7. Conclusion

We depended in adversary detection and localization on Importance Sampling-based Maximum Likelihood Joint Angle Delay Estimation (IS-based ML JADE), but in shorter time of estimation, and less complexity, and in more defined range of angles, as table 1 shows:

It was observed that the signal began to be changed its power from the angle 20 degree to angle 40, so we have to generate realizations, estimate number of paths, time delays and angle of arrivals at the range of angles from 20 to 40, so we have to:

1-scan the surrounded area defined in [−π/2,π/2] for ULAs and [0,2π] for UCAs

2-get scatterers with highest significant power and define their locations as in equation (6), depending on the distance between them and the receiver.

3-get their multipath range and range angle.

4-Generate realizations in the range of newly defined angles, estimate time delays and angle of arrivals and number of paths as in [9], but in the range of newly defined angles.

Table 1. Comparison between our method and IS-based ML JADE method

	IS-based ML JADE	Our method
Range of estimation	[0,2π]	[20,40]
Number of estimation times at worst case	(2π/($\hat{\hat{\alpha}}_{q.MLE}^{[m]}$ =5))=72 estimation times	(20/($\hat{\hat{\alpha}}_{q.MLE}^{[m]}$ =5))=4 estimation times only
Root Mean Square error calculation times (for time delays and Angle of arrival)	$\hat{\hat{\alpha}}_{q.MLE}^{[m]}$ =5 $\hat{\hat{\alpha}}_{q.MLE}^{[m]}$ =10 . . . $\hat{\hat{\alpha}}_{q.MLE}^{[m]}$ =40 (40 times)	$\hat{\hat{\alpha}}_{q.MLE}^{[m]}$ =20 $\hat{\hat{\alpha}}_{q.MLE}^{[m]}$ =25 . . . $\hat{\hat{\alpha}}_{q.MLE}^{[m]}$ =40 (20 times only)

The proposed solution studied the case of launching the jamming while MAC address spoofing taking into consideration the range and anglerange, and directionality. In some researches, the attack detection by the QOS degradation was studied. Specification (like the bit error rate and throughput) that mainly depends on the protocol used to launch the communication process at the data link layer was used to infer the influence of the attack on the communication process. These observations can be assessed by measuring downlink flooding of the spoofed stream of frames. But we used Angle of Arrival **localization** and directionality of vectors at the physical layer, to localize the adversary, while overcoming of drawbacks of other detection and localization techniques that were discussed above . The trade off may come from the time elapsed to begin the operation of the detection system, but if we ensured that it would begin with the communication process, it would give better results.

8. Acknowledgement

This work was supported in part by National Telecommunication Institute (NTI).

References

[1] Aiman Abu Samra and Ramzi Abed, “Enhancement of passive MAC spoofing Detection Techniques,” International journal of advanced Computer science, Vol. 16, No. 5, 2009.

[2] Yang, Jie. Yingying (Jennifier) Chen, Wade Trappe, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks”, IEEE transactions on parallel and distributed systems, Vol. 24, No. 1, pp.44-58, 2013.

[3] Alessandro E.C. Redondi, Matteo Cesana *, “Building up knowledge through passiv WiFi probes”, Elsevier, computer communications, Vol. 117, pp.1-12,2018.

[4] Ana Alejos, “Estimation of the Reception Angle Distribution Based on the Power Delay spectrum or Profile”, International journal of antennas and propagation, 2015.

[5] Jingya Yang, Bo Ai, Danping He, Xue Lin, Bing Hui, Junhyeong Kim, Andrej Hrovat, “A Geometry-Based Stochastic Channel Model for the Millimeter-Wave Band in a 3GPP High-Speed Train Scenario”, IEEE transactions on vehicular technology, Vol. 67, No. 5, pp. 3853-3865, 2018.

[6] Mohammed Reza Abedi, Nader Mokari *, Hamid Saeedi , “How to manage resources to provide physical layer security: Active versus passive adversary”, physical communication science direct, Vol. 27 , pp.143-149, 2018.

[7] Rupinder Cheema, Divya Bansal, Dr. Sanjeev Sofat, “Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks”, International journal of computer applications, Vol. 23, No. 7, pp. 7-15, 2011.

[8] P. Ramesh Babu, D.Lalitha Bhaskari, CH.Satyanarayana, “A Comprehensive Analysis of Spoofing”, International journal of advanced computer science and applications, Vol. 1, No 6, pp. 157-162, 2010.

[9] Faouzi Bellili, Souheib Ben Amor, Sofiène Affes, Senior Member, IEEE, and Ali Ghrayeb, Senior Member, IEEE, “Maximum Likelihood Joint Angle and Delay Estimation from Multipath and Multicarrier Transmissions With Application to Indoor Localization Over IEEE 802.11ac Radio”, IEEE International Conference on Acoustics, Speech And Signal Processing, Vol. 18, No. 5, pp. 1116-1132, 2018.

[10] John Arpee, Stan Gutowski, Mustafa Touati, “Apparatus and method for geostatistical analysis of wireless signal propagation US 6711404 B1”, U.S. Patent No. 6,711,404. 23 Mar. 2004.

[11] Yi Han, Erich P. Stuntebeck, John T. Stasko, Gregory D. Abowd, ”A Visual Analytics System for Radio Frequency Fingerprinting-based localization”, IEEE Symposium on Visual Analytics Science and technology, Atlantic City, NJ, USA pp. 35-42, 2009.

[12] Bandar Alotaibi* and Khaled Elleithy, “A New MAC Address Spoofing detection Technique Based on Random Forests”, Vol. 16, No. 3, 2016

[13] li Qing,”GIS Aided Radio Wave Propagation Modeling and Analysis”, Virginia Tech, 2005.

[14] Djamal E.Berraki, Simon M.D. Armour, Andrew R. Nix, “Benefits of sparsity of mm wave outdoor spatial channels for beamforming and interference cancellation”, physical communication, science direct, Vol. 27, pp.170-180, 2018.

[15] Balasem. S.S *, S.K.Tiong, S. P. Koh,, “Beam forming Algorithms Technique by Using MVDR and LCMV”, World applied Programming (WAP), Vol. 2, No. 5, pp. 315-324, 2011.

[16] http://en.wikipedia.org/wiki/Beamforming

[17] M.N. Hindia, A.M. Al-Samman, T.A. Rahman, T.M. Yazdani, “Outdoor Large-Scale path loss characterization in an urban environment at 26, 28, 36, and 38 GHz”, physical communication, science direct ,Vol. 27, pp.150-160, 2018”.

[18] Anton Grafstrom, Lina Schelin, “How to Select Representative Samples”, Scandinavian Journal of Statistics, Vol. 41, No.2, pp. 277-290, 2014.

[19] Craig Partridge, David Cousins, Alden W. Jackson, Rajesh Krishnan, Tushar Saxena, and W. Timothy Strayer, “Using Signal Processing to analyze Wireless Data Traffic”, ACM workshop on Wireless security – WiSE 02, pp. 67-76, 2002.

[20] https://www.sabanciuniv.edu/mdbf/telecom/eng/comnet/cisco/smart.htm

[21] https://www.sabanciuniv.edu/mdbf/telecom/eng/comnet/cisco/overview.htm

[22] David Li, "A Novel and Versatile Parabolic Reflector that Significantly Improves Wi-Fi Reception at Different Distances and Angles", Journal of Wireless Networking and Communications, Vol. 3, No. 2, pp. 13-17,2013

[23] I-Kang Fu, Chi-Fang Li, Ting-Chen Song, Wern-Ho Sheen, “Correlation Models for Shadow Fading Simulation”, IEEE C802. 16m–07/060, Tech. Rep, 2007

[24] Guerroumi, Mohamed, et al. "On the medium access control protocols suitable for wireless sensor networks- a survey." International Journal of Communication Networks and Information Security, Vol. 6, No. 2, pp. 89-103, 2014