IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 11, 2020, accepted May 25, 2020, date of publication June 2, 2020, date of current version June 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2999455

Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency

YAOQI YANG[1], (Student Member, IEEE), XIANGLIN WEI[2], (Member, IEEE), RENHUI XU[3], LAIXIAN PENG[3], LEI ZHANG[3], (Member, IEEE), AND LIN GE[1], (Student Member, IEEE)

[1]Graduate School, Army Engineering University of PLA, Nanjing 210000, China
[2]63rd Research Institute, National University of Defense Technology, Nanjing 210007, China
[3]College of Communications Engineering, Army Engineering University of PLA, Nanjing 210000, China

Corresponding author: Laixian Peng (lxpeng@hotmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61671471 and Grant 61601512, and in part by the Natural Science Foundation of Jiangsu Province under Grant BK20160770.

ABSTRACT As a promising communication paradigm in the 5G era, IEEE 802.11ad 60GHz mmWave communication has many desirable properties, including high bandwidth, narrow beam, high transmission quality, and low mutual-interference. However, recently revealed Man-in-the-middle (MITM) attack can endanger the security and privacy of mmWave communication systems. Existing MITM attack detection solutions, established on ideal assumptions, neglect the fact that a MITM attacker can change its transmitting power and make it hard to be detected. In this backdrop, a cross-layer location consistency-based MITM detection and localization algorithm is introduced in this paper. Firstly, we propose a positioning algorithm based on the information of the physical layer with a directional antenna sector propagation model; secondly, based on the information at the MAC layer, we propose a MITM attack detection scheme and a sector consistency check algorithm; thirdly, a MITM attack detection and localization algorithm using cross-layer information is proposed. Simulation results have shown that the proposed algorithm can effectively detect the MITM attack and its positioning error is less than 0.53m in typical parameter settings.

INDEX TERMS Millimeter-wave communication, man-in-the-middle attack, detection, cross-layer.

I. INTRODUCTION

The proliferation of bandwidth-intensive applications, like high-definition video, virtual reality, and argument reality, has drawn pressing need for indoor mmWave communication systems. IEEE 802.11ad, which is released as a promising technology, aims to support multi-gigabit-per-second throughput through utilizing 60GHz unlicensed frequency, and thus to support the aforementioned applications. Compared with other IEEE 802.11 standards [1], the introducing of mmWave communication in IEEE 802.11ad has many desirable characteristics, including wide available spectrum range and large information capacity; achieving narrow beam and high gain antenna easily; high resolution and strong directivity; strong ability to penetrate plasma; high transmission rate and completely free spectrum resources [2]–[7]. However, IEEE 802.11ad still faces diverse security threats,as revealed recently in [8], especially the man-in-the-middle (MITM attack), in which an attacker could hijack the information exchanged between two victims through establishing a relay path between them.

Steinmetzer *et al.* have shown the feasibility of utilizing the beam-training period for launching MITM attacks in [9]. An attacker located between the transmitter and the receiver kept listening to the channel tries to establish a relay path between the two ends; then all the transmitted packets between two victims need to be received, analyzed, and relayed by the attacker. MITM attacks could degrade legitimate communications in three aspects: first, the original legitimate communication path is changed after the attack, which will introduce extra communication delays; second, the attacker will intercept and steal the original data when the attack is performed; third, the data content may be modified by the attacker.

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenhui Yuan.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

Detecting and locating MITM attacks accurately in a timely manner is critical for restoring network service and preventing privacy leakage [9]–[13]. Steinmetzer *et al.* [9] have proposed four schemes that can be used to detect MITM attacks: detection of frequent of beam switching, detection of change of signal strength, detection of beam gap length, beacon value detection. However, in general, the above methods all need to determine a threshold in advance before conducting MITM detection, which requires a long training, and the algorithm proposed by the author can only detect whether there is a MITM attack, while it cannot locate the attacker. Wei *et al.* have proposed a location consistency-based MITM attack detection algorithm from the perspective of MAC layer [8]. However, on the one hand, the algorithm proposed by the author can only determine whether there is a MITM attack, and it cannot achieve positioning, on the other hand, the success of their proposal relies on three ideal assumptions: first, a legitimate node can accurately estimate the distances to its neighbors; second, there are at least two common neighbors between the victims for checking location inconsistency; third, legitimate nodes' coordinate systems are synchronized in advance. These assumptions limit the applicability of the algorithms presented in [8].

In this backdrop, this paper aims at tackling these problems utilizing the physical-layer as well as MAC layer knowledge. On the one hand, the algorithm proposed in this paper can detect the MITM attack; on the other hand, the algorithm can also locate the attacker at the same time, which is not considered by previous works. Therefore, this paper solves the problem of simultaneous detection and localization in the MITM attack research. Firstly, with the help of physical layer information, we establish a multi-path channel propagation model and a directional multi-sector antenna propagation model, and proposed a positioning algorithm so that the distance and relative angle between any two transceivers can be determined. Secondly, we complete the sector consistency check with the help of MAC layer information to determine the existence of a MITM attack. Thirdly, a MITM attack detection and localization algorithm based on cross-layer location consistency is put forward.

The remaining of this paper is organized as follows. Section II introduces the background and related work. In Section III, we present the MITM detection and localization algorithm. In Section IV, a series of experiments are conducted to verify the feasibility and effectiveness of the algorithm. Finally, a brief conclusion of this work is provided in section V.

II. BACKGROUND AND RELATED WORK

A. BEAM TRAINING IN IEEE 802.11ad

To maximum the transmitting gain at the transmitter as well as the received signal strength at the receiver, a beam training process is introduced in IEEE 802.11ad to help each legitimate node find its best transmitting and receiving sector numbers for each neighbor. Afterwards, the training results could be stored in a table, such as the beamforming information (BFI) table defined in reference [8], [15]; then, the upcoming transmission will be conducted according to the sector numbers stored in the BFI table.

B. MITM ATTACK

As shown in Fig.1 and Fig.2, an attacker can forge the BFI table to change the legitimate communication sector of the transmitter and receiver, thereby implementing a MITM attack.This method first assumes that the attacker must not be on the line-of-sight propagation path of the transmitting and receiving ends. At the same time, the attacker has no collaborators. The attacker finds the sector with the highest signal strength by implementing all-round monitoring, and sends counterfeit sector scan feedback to the other party. Specifically, the deception can be achieved by responding faster or blocking legitimate beams. Further, the attacker may inject fake scan feedback during the training phase to hinder the legitimate communication process. Once the fake scan feedback arrives before the feedback responded by the legitimate receiving antenna, the transmitter's antenna sector will be directed to the attacker rather than the intended receiver. After that, the attacker can act as a middleman between the transmitting and receiving ends, and the original communication mode that only gets through the transmitting and receiving ends has changed to the middleman mode [14], [16]. This is the principle of MITM attack by beam deception.

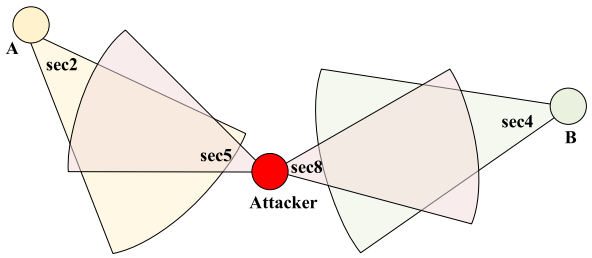


FIGURE 1. A typical MITM attack scenario.

Dest.	From	To
A	0	0
B	5	2
C	4	8

(a) A's BFI Table

Dest.	From	To
A	8	4
B	0	0
C	2	6

(b) B's BFI Table

Dest.	From	To
A	8	4
B	6	2
C	0	0

(c) C's BFI Table

FIGURE 2. Established BFI tables.

C. ToA-BASED DISTANCE ESTIMATION

ToA means the ''arrival time''. This positioning method based on ToA principle is achieved through multiple communications between the transmitting end and the receiving end [17], as shown in Fig. 3. Device A first sends a packet to device B, and records the current time information of device A and records it as T_1. After receiving the information, device B returns an ACK. After receiving the ACK, device A records the current time information and records it as T_2. At this time, the time difference is calculated according to (1), and the distance is calculated according to (2), where c is the speed of light. It should also be emphasized that T_{prop} is the processing delay, that is, the time between unpacking and packaging after receiving the package. Although the size of T_{prop} is negligible when compared to the size of T_{round}, it should be noted that T_{prop} actually exists [18]. The calculation equation and model of the distance estimation principle are as follows:

$$T_{round} = T_2 - T_1 \cdot \tag{1}$$

$$d = c \times \frac{T_{round}}{2} \cdot \tag{2}$$

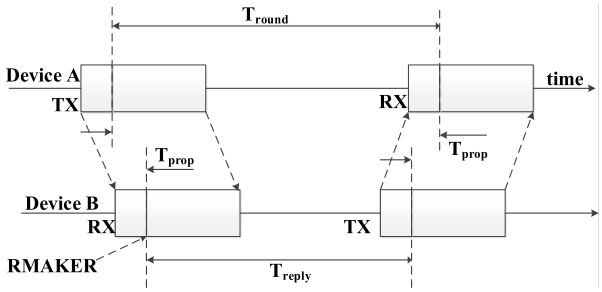


FIGURE 3. Distance estimation between two devices.

D. AoA-BASED ARRIVAL ANGLE ESTIMATION

AoA refers to the angle of arrival of a signal [19]. Based on the calculation of the distance between two adjacent antennas [20], the angle of arrival of the signal can be estimated. The model of the angle estimation principle is shown in Fig.4.

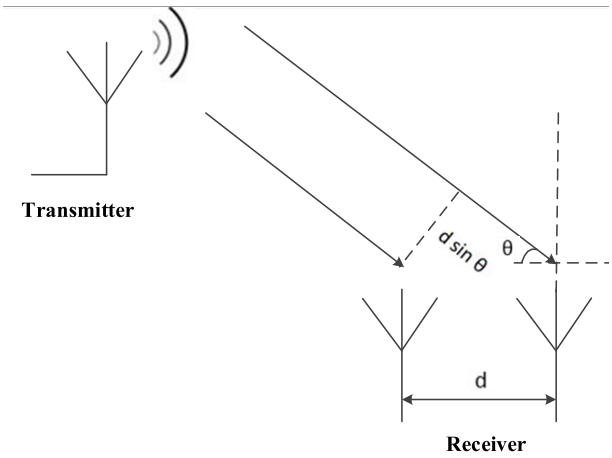


FIGURE 4. Angle estimation using antenna array.

When τ indicates the transmission time, d indicates the distance between two adjacent antennas, v indicates the speed of light, and θ indicates the angle at which the signals arrive. The transmission time τ can be calculated as follows:

$$\tau = \frac{d \cdot \sin\theta}{v} \cdot \tag{3}$$

Denote φ as the phase difference received by adjacent antennas, and ω as the angle frequency of the transmitted and received signals. The phase difference φ can can be derived as follows:

$$\varphi = w \cdot \tau \cdot \tag{4}$$

As λ indicates the wavelength of the signal, f_0 indicates the center frequency of the transmission system, and f indicates the frequency of the transmitted and received signals. The arrival angle θ can be estimated as follows:

$$\theta = \arcsin \frac{\varphi \cdot \lambda \cdot f_0}{2\pi \cdot d \cdot f} \cdot \tag{5}$$

III. MITM DETECTION AND LOCALIZATION

A. PROBLEM STATEMENT

The scenario we considered is illustrated in Fig. 1, in which the attacker has changed the original legaitimate communication path by forging sector scan feedback, and can intercept, steal or even modify the data on the legitimate path. We make an assumption that the attacker is powerful enough to crack the packets transmitted between the victims, and could distort the BFI tables exchanged by them. Then, the problem is how can a legitimate node find the existence of the MITM attacker and determine the attacker's location. Noting that the MITM attack is not on the line-of-sight propagation path of the transmitting and receiving end; the attacker has no collaborator; the MITM attack can change its transmitting power to ensure that the signal strength at the receiving end remains the same, making itself more difficult to be found.

B. BASIC IDEA

The physical-layer consistency is not considered by Wei *et al.* in [8] although they have utilized the location-consistency from the MAC-layer perspective. Actually, using only the information at the MAC layer can only detect MITM attacks with that assumption that there must be a common neighbor between legitimate transmitter and intended receiver, so it is impossible to determine the location of the attacker. Combining the knowledge of the physical layer and the MAC layer, we can not only improve the accuracy and success rate of detection, but also locate the attacker.

Therefore, to detect and locate a MITM attack, we treat the algorithms presented in [8] as a starting point, and conduct the following steps in this paper. As is shown in Fig.5. First, to facilitate the relative position estimation between any two transceivers in the physical layer, including the distance and relative angle between the two ends, a multi-path channel transmission model and an antenna sector coefficient

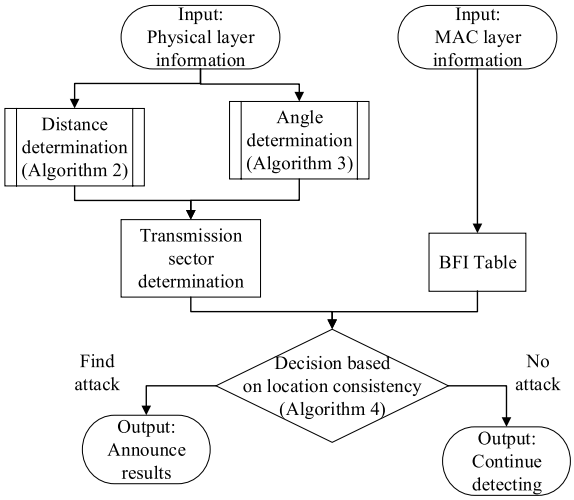


FIGURE 5. The overall diagram of the MITM detection and localization process.

model are built to determine the sector transmission function (as detailed in Section III-C). Second, in combination with the information of BFI table, a scheme of the attack detection based on MAC layer information is proposed (as detailed in Section III-D). Third, a detection and localization algorithm based on cross-layer information is proposed.

Moreover, to facilitate the description of the models and algorithms below, the notations used in this section are listed in Table 1.

TABLE 1. Notations.

Notation	Description
$A.M_A$	The matrix of antenna sector and channel
τ	The time delay in a transmission in a process
φ	The phase difference between adjacent antennas in the antenna array
θ	The relative angle between any two antennas(if θ= an empty set ϕ ,it indicates that no attack was detected)
D	The distance between adjacent antennas in the antenna array
C	The detecting results: $C = \{0, 1\}$.0 indicates that no MITM attack was detected, 1 indicates that a MITM attack was detected
T	The transmitted training sequence signal
R	The received training sequence signal
N_T	The number of sectors of directional antenna in the transmitting end
N_R	The number of sectors of directional antenna in the receiving end
V	The signal propagation speed indoors
ω	The angular frequency of signal
f_0	The central frequency of the OFDM communication system
$BFIT$	The beamforming table information in MAC layer
P	The antenna beam pattern
S	The distance between any two transmitting and receiving antennas(if S = an empty set ϕ,it indicates that no attack was detected)
β	The decision threshold based on location consistency
d_1	The distance between the attacker and node A
d_2	The distance between the attacker and node B
θ_1	The relative angle between the attacker and node A
θ_2	The relative angle between the attacker and node B
sec	The sector used by directional antennas

C. TRANSMISSION SECTOR AND LOCATION ESTIMATION BASED ON PHYSICAL LAYER INFORMATION

In order to determine the distance between the transmitting and receiving end, we establish the transmitter model, the multi-path transmission function model, and the antenna sector coefficient model, and propose a distance estimation algorithm between the transmitting and receiving antennas (see Algorithm 2 in Section III-C); for the purpose of determining the relative angle between the transmitting and receiving end, based on the AoA angle estimation principle, a relative angle estimation algorithm between the transmitting and receiving antennas is proposed (see Algorithm 3 in Section III-C).

1) ESTIMATION OF THE DISTANCE

To determine the distance between the transmitting and receiving antennas, the channel transmission function and the sector coefficient of the antenna need to be determined. In order to determine the transmission function of the system, we model the transmitter part and the indoor channel part; in order to determine the antenna sector coefficient, we establish an antenna sector transmission model and propose an antenna sector transmission function estimation algorithm (see Algorithm 1 in Section III-C); finally, based on ToA distance estimation principle, we have realized the distance estimation.

a: DETERMINATION OF THE TRANSMISSION FUNCTION

Based on the convolution theorem in time domain, and utilizing the transmitting and receiving sequences waveforms of the frequency domain, a transmitter model and a multi-path transmission model are established.

Transmitter Model: We assume that there are N antennas at the transmitting end. The signal on the transmitting antenna array is denoted as $x(t)$. After serial-parallel transformation and constellation mapping, the signal transmitted by the i-th antenna at the transmitting end is represented as $x_i(t)$. In OFDM systems, the modulation is performed by IFFT. The signal is then sent to a multi-path channel for transmission after digital-to-analog conversion [21]. The processing flow at the transmitting end is shown in Fig. 6.

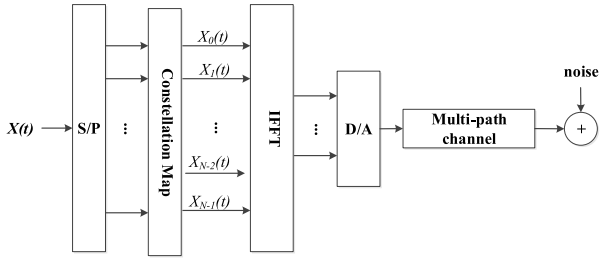


FIGURE 6. Signal processing at the transmitter end.

Indoor Multi-Path Channel Model: The effect of Doppler spread in indoor environment of millimeter wave communication is extremely small and can be ignored [22]. Therefore, when modeling indoor multi-path channels,

we only consider the fading and delay factors. The indoor multi-path environment part in Fig.7 shows the propagation process of indoor signals. When signal is transmitted from the transmitting end, it would finally reach the receiving end through multiple paths such as refraction, reflection, and line-of-sight propagation. The paths of the reflection and refraction parts are all called NLoS propagation paths.

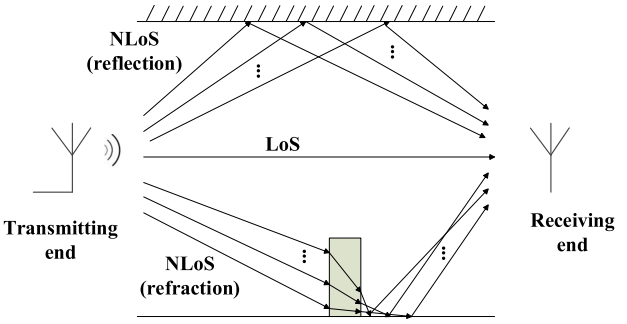


FIGURE 7. Indoor multi-path channel environment.

As is shown in Fig.7, we make an assumption that the number of indoor multi-path is l. To facilitate the analysis, we choose l as 6 [22]. The transmitting end transmits 6 different signals in sequence, denoted as $x_1, x_2, \ldots, x_6$. By detecting the spectrum of the transmitted signal and inverse Fourier transform, the corresponding amplitude $a_1, a_2, \ldots, a_6$ and phase $\theta_1, \theta_2, \ldots, \theta_6$ information of the transmitted signal can be obtained. For the receiving end, it receives the 6 signals in turns. By detecting the spectrum of the received signal and inverse Fourier transform, the corresponding amplitude $b_1, b_2, \ldots, b_6$ and phase $\omega_1, \omega_2, \ldots, \omega_6$ information of the received signal can be obtained as well.

According to the convolution theorem in time domain, when $x_i(t)$ represents the transmitting signal, $h_i(t)$ represents the impulse response signal, $y_i(t)$ represents receiving signal, $\otimes$ represents the convolution operation, we can know:

$$x_i(t) \otimes h_i(t) = y_i(t) \cdot \tag{6}$$

In this way, the signal attenuation and delay parameter information, that is, the amplitude and phase information of each path can be determined.

Considering that ambient noise is added to the model. Under the condition of AWGN (Additional White Gaussian Noise), a coefficient matrix K is introduced here. The coefficient matrix K can weight the transmission function on each path. The weighting coefficient can be determined by the minimum mean square error criterion. By optimizing the magnitude of the transmission function of each path, we can reduce the influence of white Gaussian noise on the transmission function and influence between adjacent channels. Therefore, the accuracy and reliability of the multi-path transmission function H are improved. Here, K is defined as:

$$K = \begin{pmatrix} k_{11} & \cdots & k_{16} \\ \vdots & \ddots & \vdots \\ k_{61} & \cdots & k_{66} \end{pmatrix} \cdot \tag{7}$$

Among them, k_{ij} represents the coefficient for i-th transmitted signal on j-th transmitting path. After adding noise and considering the influence between adjacent channels, the original transmitted signal X_M becomes X'_M, and σ_{ij} represents the difference between X'_M and X_M for i-th transmitted signal on j-th transmitting path.

$$X'_M - X_M = \begin{pmatrix} \sigma_{a1} & \cdots & \sigma_{f1} \\ \vdots & \ddots & \vdots \\ \sigma_{a6} & \cdots & \sigma_{f6} \end{pmatrix} \cdot \tag{8}$$

$$\begin{cases} X_M \cdot H = C^T \\ X'_M \cdot K \cdot H = C'^T \end{cases} \tag{9}$$

The minimum mean square error criterion is used to solve the coefficient matrix K, where C represents the parameter matrix of the received signal corresponding to the transmitted signal X. At this time, we can find K to minimize $\left|C'^T - C^T\right|^2$:

$$\begin{aligned} \min_K \left|C'^T - C^T\right|^2 &= \left|X'_M \cdot K \cdot H - X_M \cdot H\right|^2 \\ &= \left|X'_M \cdot K - X_M\right|^2 \cdot |H|^2 \end{aligned} \tag{10}$$

To be specific,the establishment of (10) is equivalent to the establishment of (11), from a'_j to f'_j in turns represents the first to sixth transmitted signal's amplitude on the j-th transmitted path.

$$\left| \begin{pmatrix} k_{11} & \cdots & k_{16} \\ \vdots & \ddots & \vdots \\ k_{61} & \cdots & k_{66} \end{pmatrix} \cdot \begin{pmatrix} a'_1 + \sigma_{a1} & \cdots & f'_1 + \sigma_{f1} \\ \vdots & \ddots & \vdots \\ a'_6 + \sigma_{a6} & \cdots & f'_6 + \sigma_{f6} \end{pmatrix} - \begin{pmatrix} a'_1 & \cdots & f'_1 \\ \vdots & \ddots & \vdots \\ a'_6 & \cdots & f'_6 \end{pmatrix} \right|^2 \tag{11}$$

Finally, the optimized multi-path channel transmission function $\widehat{H}$ is derived, it can be expressed as:

$$\widehat{H} = K \cdot H = K \cdot X^{-1}{}_M \cdot C^T \cdot \tag{12}$$

b: ANTENNA SECTOR TRANSMISSION MODEL

We can regard a directional antenna as a special form of omnidirectional antenna, that is, an omnidirectional antenna with a limited number of sectors with weighting coefficients. The weighting coefficient at this time depends on the antenna pattern. In order to determine the weighting coefficient of each sector in the omnidirectional antenna, we give each sector a certain weighting cofficient. Only when the weighting coefficient conforms to the content of the BFI Table, the modulus value of the product of the system transmission function is the largest. Fig.8 shows a scenario of directional antenna communication using 8 sectors.

As Fig.8 shows, if the scanning range of antenna A is divided into 8 parts, we can say that antenna A has 8 sectors,

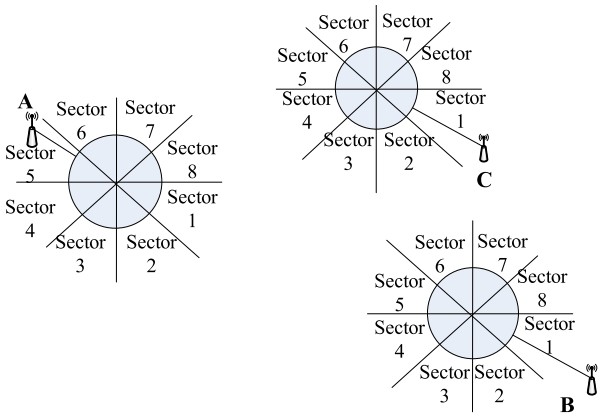


FIGURE 8. 8-sector directional antenna communication scenario.

the sector transmission function of directional antenna at each transmitting node can be expressed as:

$$\begin{aligned} &a_1M_1 + a_2M_2 + \ldots + a_8M_8 \\ &\quad = [a_1, a_2 \ldots, a_8].[M_1, M_2 \ldots, M_8]^T \\ &\quad = A.M_A \end{aligned} \tag{13}$$

where a_i represents the weighting coefficient of each sector, M_i represents the system transmission function corresponding to each sector, and i, j represents the value of the number of antenna sectors correspondingly. Similarly, for the directional antennas B and C, the weight coefficients b_i, c_i of the sectors of the antennas B and C are sequentially expressed. The coefficients of each sector must meet the contents of the antenna beam pattern and the BFI Table (as shown in Fig.2), namely:

$$\begin{cases} \max\limits_{1\le i,j\le 8} \{a_ic_j\} = a_8c_4 \\ \max\limits_{1\le i,j\le 8} \{c_ib_j\} = c_2b_6 \\ \max\limits_{1\le i,j\le 8} \{a_ib_j\} = a_8b_4 \end{cases} \tag{14}$$

For the multi-path transmission part:

$$\begin{cases} M_1 = \alpha_{11} \cdot \delta(t - t_{11}) + \ldots + \alpha_{n1} \cdot \delta(t - t_{n1}) \\ M_2 = \alpha_{12} \cdot \delta(t - t_{12}) + \ldots + \alpha_{n2} \cdot \delta(t - t_{n2}) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \ldots\ldots \\ M_8 = \alpha_{18} \cdot \delta(t - t_{18}) + \ldots + \alpha_{n1} \cdot \delta(t - t_{n8}) \end{cases} \tag{15}$$

Among them, α_i represents the attenuation of the signal by each path, and t_i represents the delay of the signal by each path, and:

$$\begin{cases} \alpha_1 + \alpha_2 + \ldots + \alpha_n = 1 \\ {\alpha_1}^2 + {\alpha_2}^2 + \ldots + {\alpha_n}^2 \ge 0.9 \\ \alpha_{LoS} = \max\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \end{cases} \tag{16}$$

n indicates that a total of n path channels exist. Because when the signal transmits on the shortest distance with the LoS path, the degree of signal attenuation wit this path is minimal. Therefore, we choose the path with the largest amplitude of the transmission function as the LoS path model, and the remaining n-1 paths as the NLoS path model. 0.9 means that the energy of the n path signals in our model is not less than 90% of the total energy.

Assuming that the number of an antenna's sectors is s, we can transform equation (13) into equation (17), and equation (14) into equation (18). Among them, a_x, b_y, c_z represent the sector coefficient that conforms to BFI table under the condition of s sectors.

$$\begin{aligned} A.M_A &= [a_1, a_2 \ldots, a_s].[M_1, M_2 \ldots, M_s]^T \\ &= [a_1, a_2 \ldots, a_s]. \begin{bmatrix} \sum\limits_{i=1}^{n} \alpha_{i1} \cdot \delta(t - t_{i1}) \\ \sum\limits_{i=1}^{n} \alpha_{i2} \cdot \delta(t - t_{i2}) \\ \qquad\qquad \ldots \\ \sum\limits_{i=1}^{n} \alpha_{is} \cdot \delta(t - t_{is}) \end{bmatrix} \end{aligned} \tag{17}$$

$$\begin{cases} \max\limits_{1\le i,j\le s} \{a_ic_j\} = a_xc_z \\ \max\limits_{1\le i,j\le s} \{c_ib_j\} = c_zb_y \\ \max\limits_{1\le i,j\le s} \{a_ib_j\} = a_xb_y \end{cases} \tag{18}$$

When solving the model, combining the beam pattern of the directional antenna and the BFI Table, we can solve $\{a_i, b_j, c_k\}$ according to equation (18). Then, we can solve (6) based on the transmitting and receiving sequences, and then combining equations (15) and (16), we can derive $\{\alpha_{ij}, t_{ij}\}$.

According to the above model solving process of the sector transmission function, we propose an estimation algorithm for the antenna sector transmission function, as shown in Algorithm 1. Step 1, we derive the sector coefficients between the transceiver antennas; in step 2-3, the delay and attenuation of the multi-path channels are determined, and the antenna sector transmission function is derived finally.

c: DETERMINATION OF DISTANCE BETWEEN TRANSCEIVER ANTENNAS

Based on the results of (8) and (9), we can get the transmission function of each sector and the parameters of the LoS path. With the ToA distance estimation principle, we can estimate the distance between any transmitting and receiving antennas. The proposed distance estimation algorithm between directional antennas is shown in Algorithm 2. Step 1, the antenna sector transmission function is derived according to Algorithm 1; in step 2-4, the LoS transmission function is determined, and time delay is estimated in order. At last we calculate the distance between two transceivers.

2) ESTIMATION OF THE RELATIVE ANGLE BETWEEN TRANSCEIVER ANTENNAS

In order to determine the relative angle between the transmitting and receiving antennas, we need to know the phase

Algorithm 1 Antenna Sector Transmission Function Estimation

Input: number of transmitting antenna sectors N_T, number of receiving antenna sectors N_R, transmitted training sequence signal T, received training sequence signal R, antenna beam pattern P, $BFIT$

Output: antenna sector transmission function $A.M_A$

1: **For** each two antennas between the transmitting and receiving ends **do**
2: Determine the transmitting and receiving antenna sector coefficients based on (14) and $BFIT$
3: **For** each sector **do**
4: Determine the multi-path transmitting function of the indoor environment according to (6)
5: Determine the transmitting function on the LoS path of the indoor environment according to (16)
6: **End**
7: Calculate the parameter estimation matrix of antenna and channel part involving the sector coefficient, delay and attenuation of multi-path transmission function according to (15) and (16)
8: Through the calculation in step 6, we get $A.M_A$
9: **End**
10: Return $A.M_A$

Algorithm 2 Directional Antennas Distance Estimation

Input: number of transmitting antenna sectors N_T, number of receiving antenna sectors N_R, angular frequency ω, signal propagation speed V

Output: distance between any two antennas S

1: **For** each two antennas between the transmitting and receiving ends **do**
2: Derive $A.M_A$ based on **Algorithm 1**
3: **For** each multi-path channel **do**
4: Find the main path parameter in a multi-path channel according to (16)
5: **End**
6: Determine the time that the signal transmitted on the LoS path according to (4)
7: Calculate the distance between the transmitting and receiving antennas S using (2)
8: **End**
9: Return S

difference between adjacent antennas and other communication environment parameters. On this basis, we can estimate the angle between the transmitting and receiving antennas based on the AoA angle estimation principle.

a: DETERMINATION OF THE PHASE DIFFERENCE BETWEEN ADJACENT ANTENNAS

Using the frequency domain waveform of the signals received by adjacent antennas, based on the inverse Fourier transform principle, the phase difference $\Delta\theta$ of the signals received by adjacent antennas can be determined.

$$2\pi \cdot e^{j\Delta\theta} \cdot \delta(\omega) \leftrightarrow e^{j\Delta\theta}. \tag{19}$$

With the known MIMO-OFDM (Multiple Input Multiple Output-Orthogonal Frequency Division Multiplexing) communication environment and the configuration of the router, we can determine the parameters such as the frequency of the transmitted signal, the center frequency, and the distance between adjacent antennas in the antenna array.

Algorithm 3 Relative Angle Between Directional Antennas Estimation

Input: number of transmitting antenna sectors N_T, number of receiving antenna sectors N_R, angular frequency ω, signal propagation speed V, center frequency f_0, distance between adjacent antennas in the antenna array D, phase difference between adjacent antennas in the antenna array φ

Output: relative angle between any two antennas θ

1: **For** each two antennas between the transmitting and receiving ends **do**
2: Determine S according to **Algorithm 2**
3: Calculate the time difference τ that the signal transmitted on the LoS path in accordance with (3)
4: Calculate the phase difference φ of the signal received by two adjacent antennas in accordance with (4)
5: Derive the relative angle θ between the transmitting and receiving antennas using (5)
6: **End**
7: Return θ

b: DETERMINATION OF THE RELATIVE ANGLE

Based on (3), (4), and (18), Algorithm 3 can estimate the relative angle between the directional antennas. Step 1, the distance between two transceivers is derived according to Algorithm 2; in step 2-4, we calculate transmission time and phase difference by turns. Finally the arrival angle is estimated successfully.

c: SECTOR NUMBER DETERMINATION

In order to conduct MITM attack detection based on location consistency, we need to determine the sector number based on the relative angle between the sender and receiver. With Algorithm 3, we can determine the relative angle between any two transmitting and receiving antennas. Using relative angles, we can further implement the determination of sector numbers. As shown by node A in Fig.8. For an 8-sector antenna, we divide the angle in a clockwise fashion, and regard a circle from sector 1 to sector 8 as 360°. For example, if the angle θ is in the range of [135°, 180°], we judge that the antenna is using sector 4 for communication.

D. MITM ATTACK DETECTION BASED ON CROSS-LAYER INFORMATION

Considering two different attack scenarios. The first scenario is one where an attacker launches an attack after legitimate communications are established. At this time, we only need to synchronize the clock between the transmitter and receiver, and record the time for legitimate communication before launching the attack. The average value is used as the legitimate communication time and the variance is used as the threshold. After the attacker initiates the establishment of illegitimate communication, the communication time between the transmitter and receiver is measured here and compared with the legitimate communication time. If the squared difference between the two recordings is no bigger than the threshold, then no attack is declared, otherwise the attack is announced.

In the second scenario, an attacker launches an attack before the time that legitimate communication is established. As shown in Fig.1, node A and node B are attacked during the communication. We can observe at the node B. With the help of Algorithm 2 and Algorithm 3, we obtain the distance d_1 and the relative angle θ_1 from the attacker to node B. From the observation at the node A, with the algorithm 2 and Algorithm 3, we obtain the distance d_2 and relative angle θ_2 between the attacker and node A. By combining the physical layer estimation information and the BFI table obtained at the MAC layer, a MITM attack decision can be made. The overall process of MITM attack detection is shown in Fig.9.

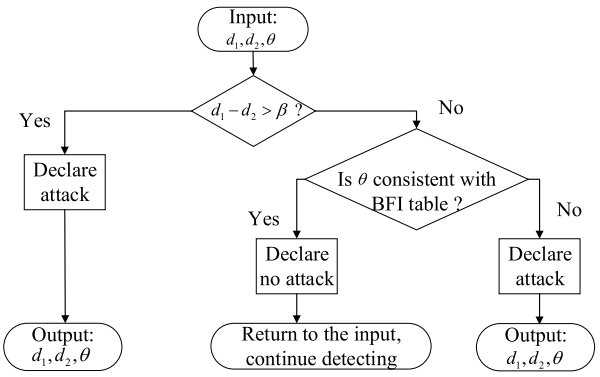


FIGURE 9. Attacker detection schematic based on cross-layer information.

From the view of distance, if there is no MITM attack, the difference between d_1 and d_2 will not exceed the decision threshold β; if there is a MITM attack, it is divided into two cases: the attacker is not on the bisector of the line connecting two communication nodes, and the attack is located on the bisector of the connection between two communication nodes. For the first case, it can still be identified by whether the difference between d_1 and d_2 exceeds the decision threshold β; the second case needs to be further judged by the relative angle and the information of the BFI Table. From the relative angle's perspective, as shown in Fig.1, we can see that the attacker has forged the sector scan feedback. To be specific, the attacker actually uses sector 5 to communicate with A, but it fraudulently responds to A that it has utilized sector 4 to communicate with you; the attacker actually uses sector 8 to communicate with B, but it fraudulently responds to B that I'm using sector 2 to communicate with you. Although this is in accordance with the contents of the BFI Table in the MAC layer, there is a contradiction in the consistency between θ and the BFI Table. Specifically, when the attacker is located on the bisector of the line connecting the two sides of the communication, from the value of θ_1 we know that the other antenna of the communication should use the sector 5 for communication. However, the feedback received by A is that the other antenna uses sector 4, so there is an inconsistency. And it would be judged that the attacker had launched an attack. Similarly, the observations on the B could also detect the attack.

In summary, the decision criteria are as follows: 1) If the difference between d_1 and d_2 exceeds the decision threshold, we announce that there is an attack; 2) If the difference between d_1 and d_2 does not exceed the decision threshold: a) θ_1 and θ_2 is consistent with the BFI table, we announce that there is no attack; b) θ_1 and θ_2 is not consistent with the BFI table, and we announce that there is an attack.

Based on the above analysis, the proposed MITM attack detection and localization algorithm based on cross-layer information is shown in Algorithm 4. Step 1, we derive the distance and arrival angle information of transceivers based on Algorithm 2 and Algorithm 3; in step 2-4, the difference between transmitting and receiving antenna are compared, and we check the consistency between arrival angle and BFI table. In the end, we get the detection and localization results.

IV. SIMULATION AND ANALYSIS

In order to verify the correctness of the algorithm, we conduct a series of experiments. Firstly we verify the correctness of the physical layer information estimation algorithm; then the validity of the MITM attack detection and localization algorithm based on cross-layer information is verified.

A. EXPERIMENTAL SETTINGS

In Section IV-B Part 1), we firstly design experiments to verify the correctness of the wireless multi-path channel transmission model, then experiment of the antenna sector transmission model is designed to verify its correctness. In the angle estimation algorithm, for the purpose of verifying the correctness of the antenna relative angle estimation algorithm, the experiment of Section IV-B Part 2) is designed.

To verify the effectiveness of the detection and localization algorithm based on cross-layer information. In Section IV-C, the method of controlling variables is used to study the effects of various experimental variables in the simulation environment. In Section IV-C Part 2), the effect of the number of antennas on the detection performance is verified. Then the effect of the number of channel paths on the detection performance is verified in Section IV-C Part 3). Section IV-C Part 4) verifies the effect of the number of sectors for

Algorithm 4 Cross-Layer Consistency-Based MITM Attack Detection and Localization

Input: number of transmitting antenna sectors N_T, number of receiving antenna sectors N_R, angular frequency ω, signal propagation speed V, center frequency f_0, distance between adjacent antennas in the antenna array D, phase difference between adjacent antennas in the antenna array φ, $BFIT$, the decision threshold β

Output: MITM attacker's results C, distance from transmitting node to attacker S_1, relative angle from transmitting node to attacker θ_1, distance from receiving node to attacker S_2, relative angle from receiving node to attacker θ_2

For each two antennas between the transmitting and receiving ends **do**
  Derive S_1, θ_1 from transmitting node based on **Algorithm 2 and 3**
  Derive S_2, θ_2 from receiving node based on **Algorithm 2 and 3**
  If $|S_1 - S_2|$ is larger than β
    Return $C = 1, S_1, \theta_1, S_2, \theta_2$
  Else
    If θ is consistent with $BFIT$
      Return $C = 0, S_1 = \phi, \theta_1 = \phi, S_2 = \phi, \theta_2 = \phi$
    Else
      Return $C = 1, S_1, \theta_1, S_2, \theta_2$
    End
  End
End

directional antenna on the detection performance. In order to obtain the positioning accuracy of the algorithm, we perform experiments of Section IV-C Part 5).

Parameter Settings: The simulation environment used in this experiment is consistent with that in [7], and the parameters are shown in Table 2.

TABLE 2. Simulation environment parameters.

Physical layer	Distance between adjacent antennas in an antenna array	10cm
	Frequency of a signal in an OFDM system	60GHz
	Number of directional antenna sectors	8/16/24/32
	Number of indoor channel paths	6/9/12
	Number of router external antennas	8/4/2
	Router model	Talon AD7200
	Antenna beam pattern	pattern2
MAC layer	Protocol type	IEEE 802.11ad

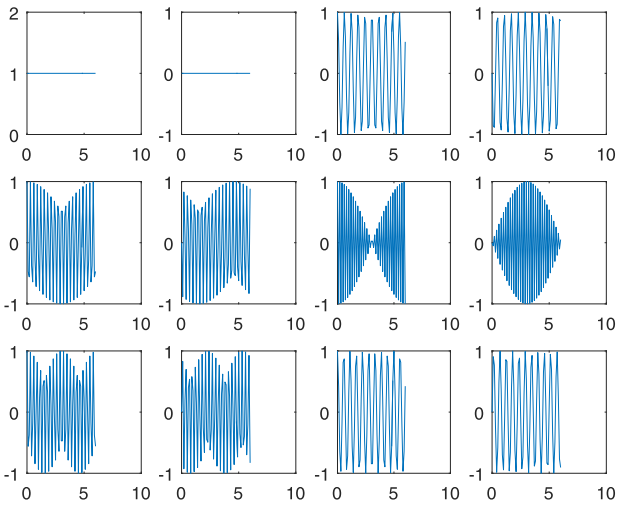
B. CORRECTNESS EXPERIMENTAL OF PHYSICAL LAYER INFORMATION ESTIMATION

1) CORRECTNESS VERIFICATION OF ALGORITHM 2

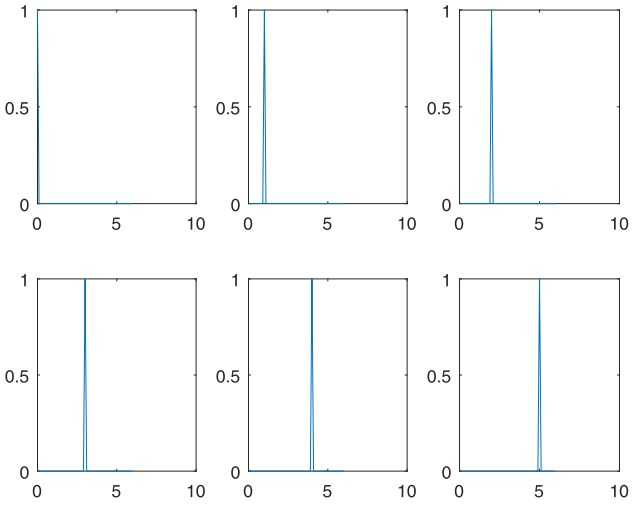
In this section, we conduct experiments to verify the correctness of the wireless multi-path channel transmission model and the antenna sector transmission model. We will test the correctness of the model from three aspects: the frequency domain waveform of the transmitting and receiving end, the frequency domain waveform of the pulse response of multi-path channel transmission function, and the spectrum of the directional antenna sector transmission function.

a: SPECTRUM OF THE TRANSMITTING AND RECEIVING SEQUENCE

Among them, Fig.10 (a) shows the waveform of the transmitted signal in frequency domain. From left to right, from top to bottom, it represents the real and imaginary images of the 6 transmitted signals in the frequency domain in turns. The horizontal axis represents the signal frequency (Hz). The vertical axis represents the signal amplitude. Fig.10 (b) shows the waveform of the transmitted signal in time domain. From left to right, from top to bottom, it represents the time-domain waveforms of the 6 transmitted signals in order. Specifically, it means that the six transmitted signals' amplitudes all are 1,



(a) Waveform of transmitting signal in frequency domain.

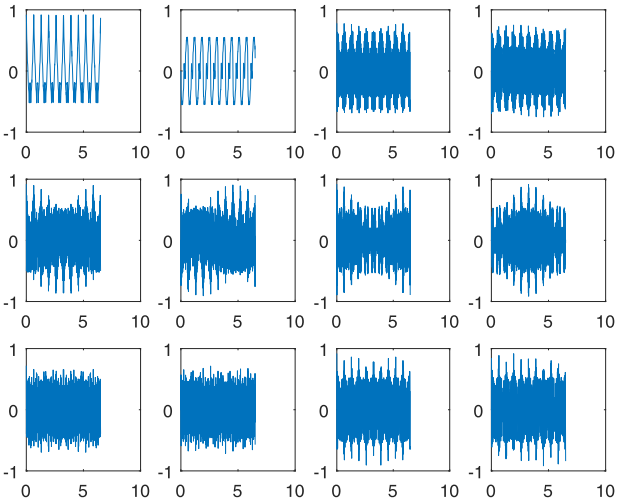


(b) Waveform of transmitting signal in time domain.

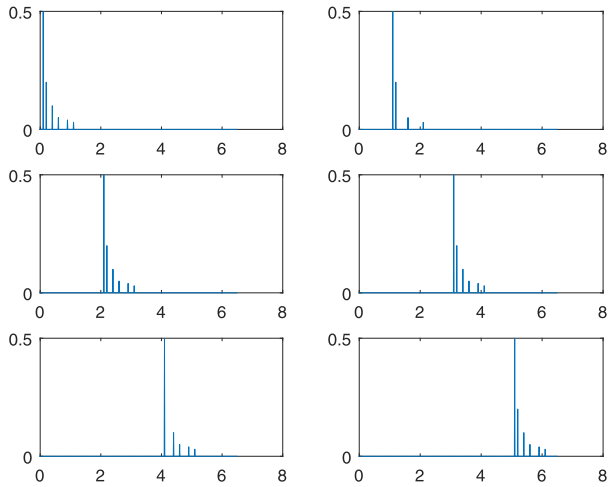
FIGURE 10. Waveform of transmitting signal in frequency domain and time domain.

and the signals' pulse impact appear on 0, 0.1, 0.2, 0.3, 0.4, and 0.5 μs in order. The horizontal axis represents time ($10^{-1}\mu s$), and the vertical axis represents amplitude.

Fig.11 (a) shows a frequency domain waveform of the received signal. From left to right, from top to bottom, the real and imaginary waveforms of the six received signals in the frequency domain are shown in order. The horizontal axis represents the signal frequency (Hz), and the vertical axis represents the signal amplitude. Figure 11 (b) shows the waveform of the received signal in time domain. From left to right, and from top to bottom, it represents the time-domain waveform of the six received signals in order. The horizontal axis represents time ($10^{-1}\mu s$), and the vertical axis represents amplitude. Specifically speaking, it indicates that the received signal is the sum of pulse impact signals. The results indicate



(a) Waveform of received signal in frequency domain.



(b) Waveform of received signal in time domain.

FIGURE 11. Waveform of received signal in frequency domain and time domain.

that the delay of each path is 0.1, 0.2, 0.4, 0.6, 0.9, and 1.1μs; the corresponding amplitude attenuation is 0.05, 0.02, 0.01, 0.05, 0.04, and 0.03.

By detecting the signal's frequency domain waveform at the transmitting end, we get Fig.10 (a), and by performing the inverse Fourier transform processing on Fig.10 (a), we get Fig.10 (b). Similarly, at the receiving end, using the principle of noise reduction in the multi-path transmission function model, we can get Fig.11 (a) and Fig.11 (b). From Fig.11 (b), it can be known that the signal received each time is the sum signals that transmitted through the multi-path. Among the signals received at the first, third, fourth, fifth, and sixth time, the number of paths for transmission is no less than five. So it indicates that the accuracy of the model is no less than 83% [22], which is consistent with our hypothesized multi-path transmission model, thus illustrating the correctness of the multi-path transmission function model.

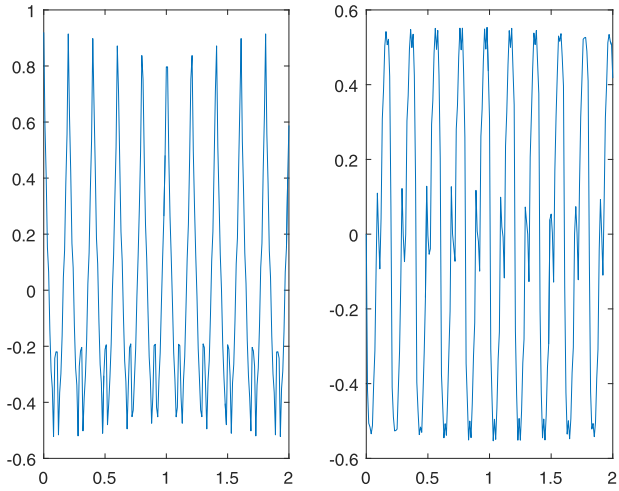
b: SPECTRUM AND WAVEFORMS OF MULTI-PATH CHANNELS

Among them, Fig.12 (a) shows a frequency-domain waveform of the multi-path channel transmission model's pulse response, and the real and imaginary parts of the multi-path transmission function are shown from left to right, the horizontal axis represents frequency (Hz), and the vertical axis represents amplitude. Fig.12 (b) shows a time-domain waveform of a multi-path channel transmission model's pulse response, the horizontal axis represents time ($10^{-1}\mu s$), and the vertical axis represents amplitude. It indicates that the delay of each path to the transmitted signal on the multi-path channel is 0.1, 0.2, 0.4, 0.6, 0.9, and 1.1μs, the corresponding amplitude attenuation is 0.05, 0.02, 0.01, 0.05, 0.04, and 0.03 in turns.

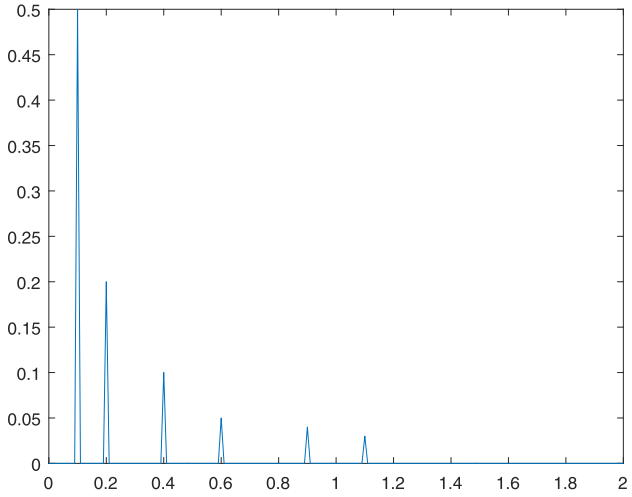
Based on the results of Fig.10 (a) and Fig.11 (a), according to the transmission principle of the communication system, it can be known that the signal received in the time domain is the result of the convolution of the transmitted signal and the system transmission function. With the help of the convolution theorem in time domain, we can obtain the frequency domain waveform of the system transmission function, as shown in Fig.12 (a). After inverse Fourier transform, a time-domain waveform of the system's transmission function is obtained, as shown in Fig.12 (b). According to Fig.12 (b), there are 6 paths when transmitting signals, which is consistent with the multi-path transmission function model we established. Each path can delay and attenuate the signal to varying degrees. The path with the largest amplitude represents the LoS path, and the remaining paths represent the NLoS paths. This is also consistent with our model, so the correctness of the multi-path transmission function model is verified.

c: SPECTRUM AND WAVEFORM OF DIRECTIONAL ANTENNA SECTOR TRANSMISSION FUNCTION

Among them, Fig.13 (a) shows the frequency domain waveform of the transmission function of each sector from node A

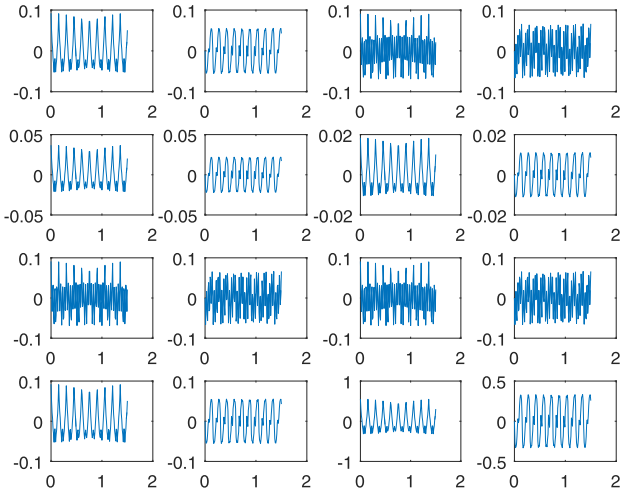


(a) Pulse response of a multi-path channel in frequency domain.

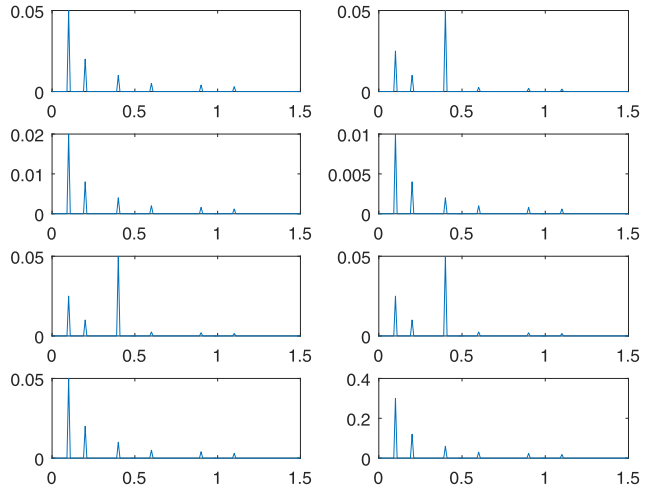


(b) Pulse response of a multi-path channel in time domain.

FIGURE 12. Pulse response of a multi-path channel in frequency and time domain.



(a) Frequency domain waveforms of the transmission function.



(b) Time domain waveforms of the transmission function.

FIGURE 13. Frequency domain and time domain waveforms of the transmission function of each sector from node A to node B.

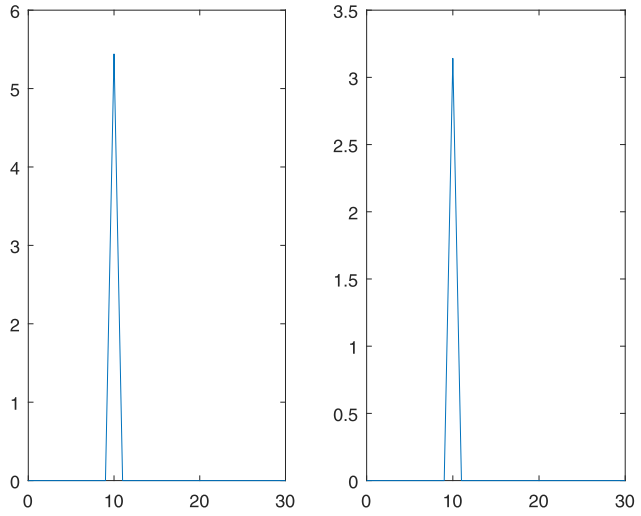
to node B. From left to right and from top to bottom, it shows the real and imaginary part, the horizontal axis represents frequency (Hz), and the vertical axis represents amplitude. Figure 13 (b) shows the waveform of the transmission function of each sector from node A to node B in time domain. From left to right and from top to bottom, the time-domain waveforms of the transmission function when using sector 1 to 8 to transmit are shown in order. The horizontal axis represents time ($10^{-1}\mu s$), the vertical axis represents the amplitude. Through comparison with Fig.12 (b), the coefficients of the eight sectors of the antenna can be calculated as 0.1, 0.05, 0.04, 0.02, 0.04, 0.05, 0.1, and 0.6 in sequence.

At the transmitting node A, sector1 to 8 is used to transmit signals in sequence, and the frequency domain waveform when each sector transmits signals is detected in order to obtain Fig.13 (a). After inverse Fourier transform of the frequency domain waveform, Fig.13 (b) is obtained. As shown in Fig.13 (b), compared with Fig.12 (b), the transmission function corresponding to each sector still conforms to the model we established, and it is expressed in the form of multiple signals. But the amplitude has changed, which means that different sector is used to transmit signals, and different paths are weighted with different coefficients. The weighting coefficient is determined by the sector and different from each other. These characteristics are consistent with the model we established, so the correctness of the model has been verified.

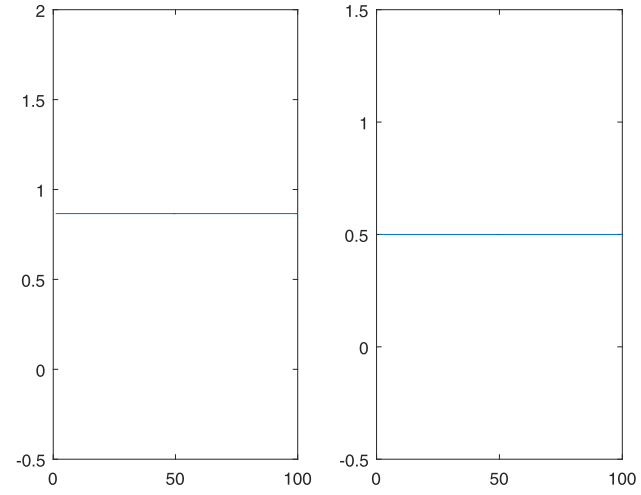
2) CORRECTNESS VERIFICATION OF ALGORITHM 3

In this section, we only need to verify the model established by the phase difference between the received signals of adjacent antennas. In accordance with equation (19), based on the inverse Fourier transform theorem, we can successfully identify the phase difference in time domain.

Among them, Fig.14 (a) shows the frequency domain waveform of the phase difference between adjacent antennas,



(a) Waveforms of phase difference in frequency domain.



(b) Waveforms of phase difference in time domain.

FIGURE 14. Waveforms of phase difference between adjacent antennas in frequency and time domain.

and the real part and the imaginary part are shown in order from left to right. The horizontal axis represents the frequency (Hz) and the vertical axis represents the amplitude. Fig.14 (b) shows a time-domain waveform of the phase difference of adjacent antennas, the real part of the phase difference $e^{j\Delta\theta}$ is shown on the left, and the imaginary part of the phase difference $e^{j\Delta\theta}$ is shown on the right. The left figure shows the modulus of the real part of $e^{j\Delta\theta}$ is 0.866, and the right figure shows the modulus of the imaginary part of $e^{j\Delta\theta}$ is 0.5.

Fig.14 (a) is obtained by considering two adjacent antennas in the antenna array and detecting the frequency domain waveforms when they transmit signals. Making inverse Fourier transform of Fig.14 (a), we obtain Fig.14 (b). According to (6), by solving the tangent value of the quotient of the imaginary part and the real part, we obtain the value of $\Delta\theta$, and thus prove the feasibility of the angle estimation algorithm.

C. PERFORMANCE VERIFICATION OF ALGORITHM 4

In Section IV-C, we firstly explain principle of the algorithm detection and positioning experiments; then we verify the performance of the algorithm from two aspects: detection rate and positioning error. Based on the control variable method, we verify the influence of the three variables of the number of antennas, the number of channel paths, and the number of antenna sectors on the detection rate of the algorithm, and at last the performance of the positioning error under different decision thresholds is verified.

1) ALGORITHM OF DETECTION AND POSITIONING PERFORMANCE EXPERIMENT

a: DESIGN OF DETECTION PERFORMANCE EXPERIMENT

Firstly, according to Algorithm 2 and Algorithm 3, we can calculate the distance and relative angle between any two transceiver ends. Secondly, according to the principle of Algorithm 4, the two nodes at the transceiver are measured in turn. If the difference between the two nodes is no larger than the decision threshold (denoted as β), then we judge that the position between two nodes is consistent. Otherwise, we judge that the MITM has launched an attack, and use the location information of the receiving end as the positioning result of the MITM attack detection. Here, we conduct a Monte Carlo simulation experiment of the MITM attacks in 500 times. When the location between the transmitting node and receiving node is inconsistent, we judge that an attack is found. After experiments of 500 times, the number of the MITM detected attacks divided by the total number of experiments will be the detection rate.

b: DESIGN OF POSITIONING PERFORMANCE EXPERIMENT

In the simulation experiment, we take an arbitrary value for the distance between any two nodes, in order to ensure the continuity of the network system work, the minimum value is 4m and the maximum value is 10m. According to Algorithm 4, we get the positioning results under different decision thresholds through experiments. Finally, we find out the relationship between threshold value and positioning error. To be specific, we can derive the positioning error in the following way. Based on the premise that the location information among the attacker, transmitting node and receiving node is given,we perform a Monte Carlo simulation experiment of the MITM attack in 500 times. Each time an attack is reported by Algorithm 4, we compare the positioning result with the attacker's real location, and use the Euclidean distance between them as the positioning error. The average of the positioning error in all cases in which the attacker is detected is used as the positioning error. The symbols involved in the simulation are shown in Table 3.

TABLE 3. Parameters.

Parameters	Meaning
α	Number of antennas in the antenna array
γ	Number of paths in a multi-path channel
ω	Number of sectors in a directional antenna
β	Threshold to detect MITM attack

2) IMPACT OF THE NUMBER OF ANTENNAS ON DETECTION PERFORMANCE

Fig.15 shows the relationship between the number of antennas and the detection performance of the algorithm under the condition that the number of sectors is 16 and the number of paths is 12. It can be seen from Fig.15 that when the decision threshold is 1.5m, the probability of detection success is 96%, 98%, and 100% in the order of the number of antennas of 8, 4, and 2. This shows that the positioning accuracy of the system remains basically the same as the number of antennas increases, so the detection success rate remains basically unchanged. The reason is that although the increase in the number of antennas has a better effect on the transmission rate of the system, in the algorithm design for detecting MITM attacks, the number of antennas cannot affect the detection and the accuracy of positioning.

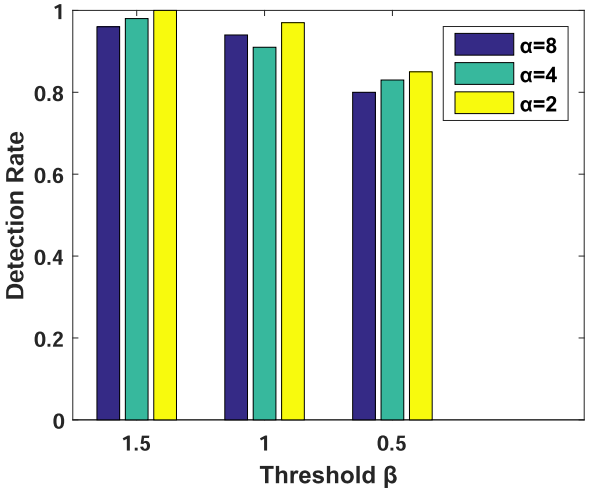


FIGURE 15. Relationship between the number of antennas and detection performance of the algorithm.

3) IMPACT OF THE NUMBER OF CHANNEL PATHS ON DETECTION PERFORMANCE

Fig.16 shows the relationship between the number of paths and the detection performance of the algorithm when the number of sectors is 16 and the number of antennas is 8. It can be seen from Fig.16 that when the decision threshold is 1.5m, the probability of successful detection is 81%, 86%, and 100% in the order of 6, 9, and 12 paths. This shows that the positioning accuracy of the system increases as the number of paths increases, so the rate of detecting successfully increases as the number of channel paths increases. The reason is that the increase in the number of channel paths can better improve the accuracy of the channel multi-path transmission function, and the mathematical model of the established multi-path channel is closer to reality. The accuracy of the transmission function of the LoS path is therefore higher. So the accuracy of distance estimation is improved, and the ability of system decision and positioning is improved.

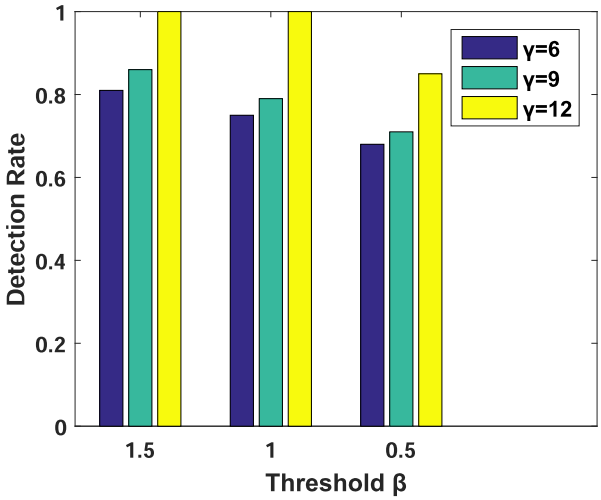


FIGURE 16. Relationship between the number of paths and the detection performance of the algorithm.

4) IMPACT OF THE NUMBER OF ANTENNA SECTORS ON DETECTION PERFORMANCE

Fig.17 shows the relationship between the number of sectors and the detection performance of the algorithm under the condition that the number of antennas is 8 and the number of paths is 12. It can be seen from Fig.17 that when the judgment threshold is 1.5m, the probability of successful detection is 82%, 100%, 100%, and 100% in the order of 8, 16, 24, and 32 sectors, which indicates that the positioning accuracy of the system increases with the number of antenna sectors increasing, so the rate of successful detection also increases.

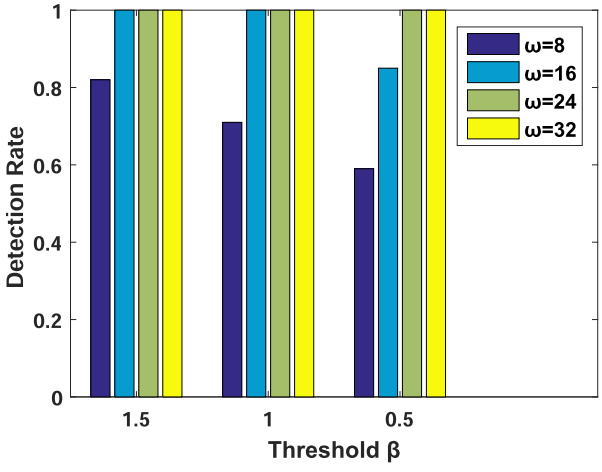


FIGURE 17. Relationship between the number of sectors and the detection performance of the algorithm.

The reason is that the increase in the number of antenna sectors can effectively improve the accuracy of the transmission function, so the accuracy of the distance estimation algorithm is improved, and the rate of successful detection is higher.

5) ANALYSIS OF SYSTEM POSITIONING ERROR

Based on Fig.17, under the condition that the number of sectors is no less than 16, the system's detection rate performance is the best. Therefore, under the condition that the number of sectors is 16, the number of paths is 12, and the number of antennas is 8. Firstly, the relationship between the algorithm detection success rate and the threshold is clarified by experiments, then we select 3 typical thresholds to further determine the positioning error of the algorithm.

Fig.18 shows the relationship between the decision threshold and the probability of successful detection. It can be seen from Fig.18 that when the decision thresholds are 0.5m, 0.6m, and 0.7m, the corresponding successful detection probability is 76%, 87%, and 100%. This shows that as the threshold increases, the probability of success detection also increases.

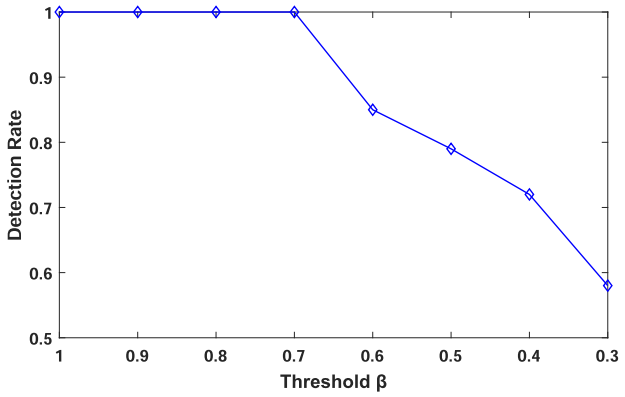


FIGURE 18. Relationship between probability of detection success and threshold.

Fig.19 shows the positioning error of the algorithm under different decision thresholds. It can be seen from Fig.19 that if the probability of successful detection is no less than 90%, when the decision thresholds are 0.7m, 0.6m, and 0.5m, the positioning error of the algorithm is 0.53m, 0.60m, and 0.69m respectively.

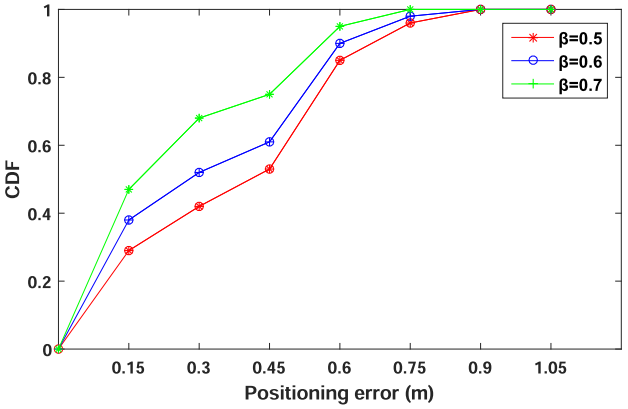


FIGURE 19. Positioning error of the algorithm.

D. DISCUSSION

On the one hand, we can know that under the typical settings, the detection rate of the algorithm proposed in this paper is no less than 90% in various scenarios, and the positioning error does not exceed 0.53m. On the other hand, because the current algorithm has multiple input parameters, the algorithm is sensitive to the parameter estimation errors, which may affect the practicability of the algorithm.

In addition, the algorithm proposed in this paper may benefit indoor-localization and jammer localization scenarios.

At last, the algorithms in this paper are designed based on the assumption that the attacker is static during the detecting process, but the position of the attacker may change in the actual environment. In order to enhance the applicability of the algorithm, the improvement of the algorithm in terms of timeliness will be our future work.

V. CONCLUSIONS

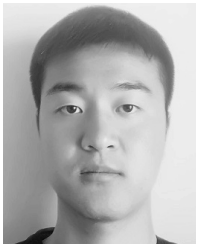
In the IEEE 802.11ad standard, directional communication has been widely used, which makes man-in-the-middle (MITM) attack a greater security risk in cyberspace. In this background, a cross layer location consistency-based on MITM attack detection and localization algorithm is presented in this paper. On the one hand, we estimate the angle and distance between directional antennas based on the physical layer information; on the other hand, we implement the consistency check of the attacker's position based on the MAC layer information; finally, we implement the detection and positioning of the MITM attacker. Our experimental results have shown that the model based on the physical layer information is correct and feasible; the performance of the MITM attack detection and localization algorithm based on cross-layer information is better, in an environment with 16 sectors, 12 paths, and a threshold of 0.7m, the typical positioning error is 0.53m, and the detection rate is no less than 90%. We make a discussion about the complexity and timeliness of the algorithm, although the algorithm proposed in this paper can detect and locate the MITM attack, the complexity and timeliness of the algorithm are still the limitations of the algorithm. In the future, the algorithm will be optimized to effectively reduce the complexity. Additionally, dynamic detection and localization of MITM attacks will make the algorithm more practical.

REFERENCES

[1] X. Wei, Q. Wang, T. Wang, and J. Fan, "Jammer localization in multi-hop wireless network: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 765–799, 2nd Quart., 2017.

[2] P. Zhou, K. Cheng, X. Han, X. Fang, Y. Fang, R. He, Y. Long, and Y. Liu, "IEEE 802.11ay-based mmWave WLANs: Design challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1654–1681, 3rd Quart., 2018.

[3] S. Balakrishnan, P. Wang, A. Bhuyan, and Z. Sun, "Modeling and analysis of eavesdropping attack in 802.11ad mmWave wireless networks," *IEEE Access*, vol. 7, pp. 70355–70370, 2019.
[4] Y. C. M. Tan, "Computational modelling and simulation to design 60 GHz mmWave antenna," in *Proc. IEEE Antennas Propag. Soc. Int. Symp.*, Toronto, ON, Canada, Jul. 2010, pp. 1–4.
[5] D. E. Berraki, S. M. D. Armour, and A. R. Nix, "Codebook based beamforming and multiuser scheduling scheme for mmWave outdoor cellular systems in the 28, 38 and 60 GHz bands," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Austin, TX, USA, Dec. 2014, pp. 382–387.
[6] M. C. Caballe, A. C. Auge, E. Lopez-Aguilera, E. Garcia-Villegas, I. Demirkol, and J. P. Aspas, "An alternative to IEEE 802.11ba: Wake-up radio with legacy IEEE 802.11 transmitters," *IEEE Access*, vol. 7, pp. 48068–48086, 2019.
[7] K. Chandra, R. V. Prasad, and I. Niemegeers, "Performance analysis of IEEE 802.11ad MAC protocol," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1513–1516, Jul. 2017.
[8] X. Wei and C. J. Tang "Location consistency-based MITM attack detection in ad networks," in *Cyberspace Safety and Security* (Lecture Notes in Computer Science), vol. 11983, J. Vaidya, X. Zhang, and J. Li. Cham, Switzerland: Springer, 2019.
[9] D. Steinmetzer, Y. Yuan, and M. Hollick "Beam-stealing: Intercepting the sector sweep to launch man-in-the-middle attacks on wireless IEEE 802.11 ad networks," in *Proc. 11th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*. New York, NY, USA: ACM, 2018, pp. 12–22.
[10] G. Jakllari, I. K. T. Broustis, S. V. Krishnamurthy, and L. Tassiulas, "Handling asymmetry in gain in directional antenna equipped ad hoc networks," in *Proc. IEEE 16th Int. Symp. Pers., Indoor Mobile Radio Commun.*, vol. 2, Sep. 2005, pp. 1284–1288.
[11] A. Akhtar and S. C. Ergen "Directional MAC protocol for IEEE 802.11ad based wireless local area networks," *Ad Hoc Netw.*, vol. 69, pp. 49–64, Feb. 2018.
[12] F. De Rango, V. Inzillo, and A. A. Quintana "Exploiting frame aggregation and weighted round Robin with beamforming smart antennas for directional MAC in MANET environments," *Ad Hoc Netw*, vol. 89, pp. 186–203, Jun. 2019.
[13] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN infrastructure of IoT–fog networks from MitM attacks," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1156–1164, Oct. 2017.
[14] A. Esfahani, G. Mantas, J. Ribeiro, J. Bastos, S. Mumtaz, M. A. Violas, A. M. De Oliveira Duarte, and J. Rodriguez, "An efficient Web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain," *IEEE Access*, vol. 7, pp. 58981–58989, 2019.
[15] B. Li, Z. Zhou, W. Zou, X. Sun, and G. Du, "On the efficient beamforming training for 60 GHz wireless personal area networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 2, pp. 504–515, Feb. 2013.
[16] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016.
[17] S. Wu, S. Zhang, and D. Huang, "A TOA-based localization algorithm with simultaneous NLOS mitigation and synchronization error elimination," *IEEE Sensors Lett.*, vol. 3, no. 3, pp. 1–4, Mar. 2019.
[18] I. Sharp and K. Yu, "Indoor TOA error measurement, modeling, and analysis," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 9, pp. 2129–2144, Sep. 2014.
[19] W. Gerok, M. El-Hadidy, S. A. El Din, and T. Kaiser, "Influence of the real UWB antennas on the AoA estimation based on the TDoA localization technique," in *Proc. IEEE Middle East Conf. Antennas Propag. (MECAP)*, Cairo, Egypt, Oct. 2010, pp. 1–6.
[20] S.-F. Chuang, W.-R. Wu, and Y.-T. Liu, "High-resolution AoA estimation for hybrid antenna arrays," *IEEE Trans. Antennas Propag.*, vol. 63, no. 7, pp. 2955–2968, Jul. 2015.
[21] R. Xu, L. Wang, Z. Geng, H. Deng, L. Peng, and L. Zhang, "A unitary precoder for optimizing spectrum and PAPR characteristic of OFDMA signal," *IEEE Trans. Broadcast.*, vol. 64, no. 2, pp. 293–306, Jun. 2018.
[22] B. Lee, S. Kwon, H. Moon, J. Lim, J. Seok, C. Mun, and Y. Yoon, "Modeling the indoor channel for the MIMO system using dual polarization antennas," in *Proc. Eur. Conf. Wireless Technol.*, Manchester, U.K., Sep. 2006, pp. 334–337.



YAOQI YANG (Student Member, IEEE) was born in Jinchang, in 1997. He received the B.S. degree from the College of Communications Engineering, Army Engineering University of PLA, in 2019. His research interests include wireless communications systems and signal processing.

XIANGLIN WEI (Member, IEEE) received the Ph.D. degree from the PLA University of Science and Technology, Nanjing, China, in 2012. He is currently working as a Researcher with the 63rd Research Institute, National University of Defense Technology, Nanjing. His research interests include mobile edge computing and wireless network optimization. He has served as an editorial member of many international journals and a TPC member of a number of international conferences.

RENHUI XU received the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 2010. He is currently an Associate Professor with the College of Communications Engineering, Army Engineering University of PLA. His research interests include integrated radar-communication systems, wireless communications systems, signal processing, and wireless ad hoc networks.

LAIXIAN PENG was born in China, in 1978. He received the B.S. and Ph.D. degrees in telecom engineering from the Nanjing Institute of Communications Engineering, Nanjing, in 1999 and 2004, respectively. Since 2008, he has been an Associate Professor with the PLA University of Science and Technology, where he was promoted to a Professor, in 2016. His research interests include high-speed switching architectures and ad hoc networks and applications. He was a recipient of the Excellence Ph.D. Thesis Award of Jiangsu Province, in 2005.

LEI ZHANG (Member, IEEE) received the Ph.D. degree from the Nanjing Institute of Communications Engineering, PLA University of Science and Technology (PLAUST), in 2000. From 2001 to 2003, he conducted his Postdoctoral Research with the National Mobile Communications Research Laboratory, Southeast University. He was an Associate Professor of communicators engineering with PLAUST, in 2003, where he was promoted to a Professor, in 2012. His major research interests include embedded operating systems, fog computing, and ad-hoc networking.

LIN GE (Student Member, IEEE) was born in Jingmen, in 1992. She received the B.S. degree in information engineering from the Institute of Communications Engineering, PLA University of Science and Technology, in 2015. Her research interest includes wireless ad hoc networks.