Abstract—This paper proposes a new channel state based secure wireless communication mechanism to realize secure communication with a pre-equalization function in a physical layer. Researches of physical layer security have been proposed to achieve secure communication in physical layers. On the contrary, there are a few issues where terminals in a same direction can receive a message, overhead due to complex control mechanisms, special hardware, etc. This paper focuses on practical wireless communication environment, where multi-path signals are received at a receiver. It is common knowledge that a channel state according to multi-path signals is different when a position of a receiver is different. The transmitter of proposed scheme transmits an optimized signal to a receiver with pre-equalizing the signal according to the channel state between the transmitter and the receiver. Therefore, only the receiver that has the same channel state for the pre-equalizing can obtain the high quality signal from the transmitter, and can demodulate the signal correctly. As a result, eavesdroppers around the transmitter cannot equalize the received signal before a demodulation process for the received signal because they exist at a different place of the receiver. The numerical results show that the proposed scheme can realize secure communication in typical wireless channel models. It means that a legitimate receiver can demodulate a signal correctly and eavesdroppers suffer from demodulation errors. As a result, we can find that the proposed scheme can utilize a channel state as an encryption key in physical layer security communication.

I. INTRODUCTION

Wireless communication has potential security risks due to its broadcast on radio signals. Therefore, eavesdroppers within communication range can intercept a signal without a risk of detection by a legitimate transmitter and a receiver. Typical wireless communication systems employ encryption technologies in upper layers such as data link layer, network layer, and application layer. Encryption technologies require a shared mechanism for an encryption key before secure communication. Typical key shared mechanisms in wireless communication have an overhead to realize a secure key exchange. As a result, physical security mechanisms, where only legitimate receiver can demodulate a signal from a transmitter, have been considered by focusing on some characteristics in physical layer [1], [2].

Basic concepts of physical security technologies are to deteriorate a signal quality of eavesdroppers comparing to that of a legitimate receiver. As a result, eavesdroppers cannot demodulate the signal correctly due to the low SNR (Signal to Noise Ratio) signal, and fail to obtain the data correctly from the signal. Conventional work typically uses SISO (Single-Input and Single-Output) systems, where one antenna transmits a signal and one antenna receives this signal. Some work employs an additional transmitter antenna to select an adequate transmitter antenna for a legitimate receiver, not for eavesdroppers [3], [4]. Recent work uses MIMO (Multiple-Input and Multiple-Output) systems to transmit a signal and an artificial noise signal from different antennas simultaneously [5], [6]. A transmitter creates an artificial noise signal according to a predefined coding mechanisms, and informs the predefined coding mechanisms to a legitimate receiver beforehand [7]. Therefore, the legitimate receiver can recognize the artificial noise signal and can remove it from the received signal to obtain a high SNR signal. On the contrary, eavesdroppers suffer from the low SNR signal because they cannot remove the artificial noise signal. Another work employs a directional signal transmission to improve a SNR at a legitimate receiver [8], [9]. Some work for practical usages considers a physical security in cellular networks [10], [11]. On the whole typical conventional work requires a modification of physical layer design to realize a special function for a physical security. Therefore, difficulty to employ conventional wireless communication devices is a big challenge in practical usages.

This paper focuses on practical wireless communication environment, where a receiver receives multi-path signals, and a channel state at a receiver changes according to its position. A channel state is well known to be different and to change independently when an antenna position is different more than a half wave length of a signal. General wireless systems try to equalize a received signal to obtain an undistorted signal from the distorted signal to obtain correct data. Our idea is to modify a signal to a receiver at a transmitter according to a channel state between the transmitter and the receiver because the channel state is a unique parameter for both terminals, and a different terminal has a different channel state. Therefore, eavesdroppers in our idea fail to demodulate the modified signal because the modified signal passes through a different channel between a transmitter and an eavesdropper, and it is still a distorted signal. As a result, only legitimate receiver can obtain an undistorted signal and can demodulate it correctly. On the contrary, the other receivers including eavesdroppers receive a signal distorted by the channel between the transmit-
ter and the receiver and the channel between the transmitter and the other receivers, and fail to demodulate it.

This paper employs a pre-equalization technique, where a transmitter modifies a signal according to a channel state to a receiver, to realize a new physical security communication. The proposal scheme uses a pre-communication mechanism, such as RTS/CTS (Request to Send/Clear to Send) in IEEE 802.11, to obtain a latest channel state for a pre-equalization technique. Then, a transmitter pre-equalizes a signal according to the channel state for a legitimate receiver. The pre-equalized signal will change to an undistorted signal by passing the channel to the legitimate receiver. Therefore, the legitimate receiver can receive the undistorted signal and can demodulate it to obtain correct data. On the contrary, receivers at a different position receive a distorted signal and fail to demodulate the signal because receivers cannot equalize the signal without the channel state information between the transmitter and the legitimate receiver. The simulation assumes the specification of IEEE 802.11a and typical multi-path fading models proposed by Joint Technical Committee (JTC). The numerical results show that only legitimate receiver can demodulate a signal correctly and obtain data, and the other receivers, that have a different channel state, fail to demodulate the signal. Additionally, the communication performance of the proposed scheme is almost same in IEEE 802.11a systems. Therefore, the proposed scheme can realize the similar communication performance with a secure communication based on IEEE 802.11a devices.

II. Secure Communication by Pre-equalization

A. Pre-equalization mechanism for physical security

The proposed secure communication scheme uses a channel state, that characterizes wireless communication performance, as a secure key because a channel state between terminals changes independently. A channel state at a same instance is almost constant when a same frequency is used for bidirectional communication. Therefore, both terminals have equal effect according to a channel state between the terminals. On the contrary, the other terminals, that exist at a different place more than a half wave length of a radio signal, have a different channel state because the channel state depends on a combination of multi-path signals. Additionally, each channel state changes independently when a position is different because multi-path condition is especially different at each position. As a result, eavesdroppers at a different position to the legitimate receiver receive the distorted signal because the signal is affected by the channel between the transmitter and the legitimate receiver, and the channel between the transmitter and eavesdroppers. Fig. 1 shows the overview of our proposed secure communication scheme with pre-equalization mechanism. The figure assumes that some terminals including an eavesdropper communicate with a transmitter with the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol. In the figure, the transmitter transmits a signal to the receiver, and the eavesdropper tries to receive the signal from the transmitter.

Fig. 1(a) shows the typical communication in wireless LAN systems. The transmitter transmits an undistorted OFDM signal to the receiver. The transmitted OFDM signal changes to the distorted signal according to the channel state $H_R$ between a transmitter to a receiver. Therefore, the receiver receives the distorted signal from the transmitter. As typical OFDM signal includes pre-defined pilot signals to estimate the channel state $H_R$, the receiver can equalize the distorted signal to the undistorted signal. Finally, the receiver can obtain the undistorted OFDM signal, and can demodulate the signal to receive the data correctly.

Fig. 1(b) shows the communication of the proposed secure communication system. The proposed scheme assumes a semi-static condition of terminals. Hence, a channel state $H_R$ between a transmitter and a receiver can be considered to be a constant during a packet period. Additionally, the channel state from the transmitter to the receiver and that from the receiver
to the transmitter are almost same because both terminals use a same frequency band. Therefore, the transmitter estimates the channel state $H_R$ by receiving a control packet such as CTS. Then, it pre-equalizes a signal according to the estimated channel state $H_R$ before a packet transmission. The pre-equalized signal will change to an undistorted signal by passing the channel to the receiver. Finally, the receiver can receive the undistorted signal from the transmitter, and can demodulate the signal without any equalization. The other receivers including eavesdroppers can also receive the signal from the transmitter. However, the channel state between another receiver and the transmitter differs from that between the receiver and the transmitter. As a result, the other receivers cannot receive the undistorted signal because the pre-equalized signal passes through the different channel $H_E$, and changes to the different distorted signal. In this case, the received signal is still distorted even if they try to equalize the signal by the channel state $H_E$. As a result, they fail to decode the received signal due to the signal distortion, and suffer from bit errors.

### B. System Model

Fig. 2 shows the frame format for IEEE 802.11a. The frame of IEEE 802.11a consists of the short preamble, the long preamble, and the continuous OFDM symbols. The first OFDM symbol conveys the control information in the physical layer and others convey the data payload. The proposed scheme assumes the frame format for IEEE 802.11a because our target is to realize a secure communication with conventional wireless devices.

Fig. 3 shows the system model of the proposed scheme. The proposed scheme assumes the typical OFDM system in IEEE 802.11a. In the proposed scheme, the data sequence is mapped in the frequency domain to create primary modulation signals in a same OFDM system manner. Then, it pre-equalizes the primary modulation signals according to the pre-estimated channel state by an exchange of control packets before the data communication. The time-domain signal can be obtained by an IFFT (Inverse Fast Fourier Transform) operation of the pre-equalized frequency-domain signal. Then, a Guard Interval (GI) against multi-path signals should be inserted same as general OFDM systems.

A receiver performs an AGC (Automatic Gain Control), signal detection, timing detection, frequency offset estimation by using a short preamble. It also estimates more accurate timing and frequency offset with a long preamble. Typical IEEE 802.11a based receiver estimates a channel state by using pilot signals in a long preamble, and equalizes the received signal to obtain the undistorted signal. On the contrary, the proposed scheme based transmitter pre-equalizes the signal of OFDM symbol parts in the frame format before a packet transmission. The proposed scheme assumes that the short and the long preamble are the same signal in IEEE 802.11a.

Therefore, the proposed scheme based receiver can detect the signal in a same manner of IEEE 802.11a. Then, it can demodulate the signal even if it does not equalize the received signal because the received signal is equalized to the undistorted signal by passing through the channel.

An eavesdropper at a different position to the receiver also receives the pre-equalized signal. However, the channel state between the eavesdropper and the transmitter differs from that between the receiver and the transmitter. Therefore, the received signal is not equalized by the channel between the eavesdropper and the transmitter, and is still a distorted signal for the eavesdropper. Additionally, the eavesdropper cannot equalize the received signal due to lack of the channel state information between the transmitter and the receiver. Then, it fails to demodulate the signal due to the distorted signal, and obtains erroneous data from the signal. As a result, the only way for eavesdroppers to demodulate the signal is to exist at the same place of the receiver.

### C. Communication signaling

The proposed scheme requires a channel state to a receiver to pre-equalize a signal. Generally, a channel state varies according to time. Therefore, a channel state should be estimated before data transmission. The proposed scheme employs the RTS/CTS mechanism to estimate a channel state because a transmitter can estimate the channel state by using a pilot signal in CTS. Additionally, ACKnowledgement packets are also used to update the estimated channel state when data packets are continuously transmitted.

### D. Pre-equalization

A data packet of the proposed scheme consists of $S$ data symbols. Each data symbol has $M$ sub-carriers. The number of FFT point is $N$, the GI length is $N_g$. As a transmitter estimates a channel state to a receiver by using a CTS packet, the pilot signal in the CTS packet is defined as $A_p(n)$, the channel state between the transmitter and the receiver is $H(n)$. The frequency-domain received signal affected by the channel $R(n)$ can be described as the following equation.

$$R(n) = A_p(n) \cdot H(n) + W(n),$$

(1)
where $W(n)$ is the additive white gaussian noise (AWGN).

The transmitter can estimate the channel state $\hat{H}(n)$ by the following equations because it knows the predefined pilot signal $A_p(n)$.

\[
\hat{H}(n) = \frac{R(n)}{A_p(n)} = A_p(n) \cdot H(n) + W(n) \\
= H(n) + \frac{W(n)}{A_p(n)},
\]

where $n$ is the sub-carrier number.

The pre-equalized signal $A_{peq}(s, n)$ is described as

\[
A_{peq}(s, n) = \frac{A(s, n)}{H(n)} (0 \leq s \leq S - 1),
\]

where $A(s, n)$ is the frequency-domain data including $M$ sub-carriers between the sub-carrier number $L_1$ and $L_2$, $\hat{H}(n)$ is the estimated channel state, $s$ is the symbol number.

In a same manner of OFDM system, both edges of the pre-equalized signal $A_F(s, n)$ should be inserted zero-padding to remove aliasing. Then, $N$ point IFFT converts $A_F(s, n)$ to $a(s, k)$ which is the time-domain signal, where $k$ is the sample number.

\[
a_{peq}(s, k) = \sum_{n=0}^{N-1} A_{peq}(s, n) \cdot e^{j \frac{2\pi k}{N}}
\]

\[0 \leq k \leq N - 1\]  (4)

The Guard Interval $a_{gi}$ consists of $N_g$ samples is added to the top of the time-domain signal $a(s, k)$ to solve an inter-channel interference due to an inter-symbol interference. The GI $a_{gi}$ can be described by the following equation.

\[
a_{gi}(s, n_g) = a_{peq}(s, N - N_g + n_g) (0 \leq n_g \leq N_g - 1)\]  (5)

The GI consists of the last part of $N_g$ samples in the time-domain signal $a(s, k)$. The GI length $N_g$ should be set according to a maximum propagation delay in an assumed communication condition.

A channel state is practically constant during a short period in quasi-static channel. In this condition, we can describe the received signal $r(s, k)$ without the GI as follows.

\[
r(s, k) = \begin{cases} 
\sum_{l=0}^{k} \rho_{peq}(s, k - l) + \\
\sum_{l=k+1}^{L-1} \rho_l(s) \cdot a_{peq}(s, N + k - l) + w(s, k) \\
\sum_{l=0}^{L-1} \rho_l(s) \cdot a_{peq}(s, k = l) + w(s, k) \\
\end{cases}
\]

\[0 \leq k \leq L - 1\]  (6)
where \( \rho_l(s) \) is a time-domain impulse response at \( s \) symbol for a \( l \)th delay, and \( w \) is an AWGN. The second part of the received signal at the condition (0 \( \leq k \leq N_g - 1 \)) means a GI. A \( N \) points FFT converts the time-domain signal \( r(s, k) \) to the frequency-domain signal \( \hat{A}(s, n) \). Finally, the demodulated data can be obtained by removing the zero padding parts as follows.

\[
\hat{A}(s, n) = \sum_{k=0}^{N-1} r(s, k) \cdot e^{-j \frac{2\pi nk}{N}} \\
A_{peq}(s, n) \cdot H(s, n) + W(s, n) \\
\frac{A(s, n)}{H(n)} \cdot H(s, n) + W(s, n) \\
\approx A(s, n) + W(s, n)
\] (7)

### III. Numerical Results

We have evaluated the secure performance of the proposed scheme with MatLab. The evaluation assumes IEEE 802.11a based wireless system, and employs the frame format of IEEE 802.11a in Fig. 2 because our target is to utilize conventional consumer devices to realize secure communication. Therefore, the frame format consists of the preamble parts and the payload part. Each OFDM symbol has 64 sub-carriers for 48 data sub-carriers, 4 pilot sub-carriers, and 12 zero-padding sub-carriers. The proposed pre-equalization is applicable only to the data sub-carriers. The proposed receiver demodulates a received packet without an equalization. We employ typical channel models proposed by Joint Technical Committee (JTC). The selected models assume an indoor channel, an outdoor channel with low antenna height, and Rayleigh fading channel that is a general multi-path channel in wireless communication. The detail channel models are described in Table I. Table I shows the assumed propagation delay and the propagation loss in each channel model. The maximum propagation delay in the evaluated channel model is shorter than the GI length not to occur an inter-symbol interference. Detail simulation parameters are shown in Table II.

Fig. 5 shows the bit error ratio performance in the conventional IEEE 802.11a system, where a receiver equalizes a received signal. The results demonstrate that the performance in JTC models has a similar performance in the Rayleigh fading environment. The reason is that performance in OFDM systems is not affected by multi-path signals within GI period. Additionally, the performance of JTC indoor residential A model has better performance comparing to those of the other environments. This is because, JTC indoor residential A model assumes a small number of multi-path signals and degradation of each multi-path signals is large. Therefore, the dominant factor for the performance is the direct signal. This means that the assumed environment of JTC indoor residential A model is similar to an AWGN environment.

Fig. 6 shows the bit error ratio performance of a legitimate receiver in the proposed scheme. The legitimate receiver requires a low bit error ratio to realize high quality communication. The results show that the performance in almost all channel models has a similar performance due to the same reason in Fig. 5. The performance in JTC indoor residential A model also has better performance according to the same reason. Additionally, the performance of the proposed scheme has a similar performance in the conventional performance. Therefore, we can find that the proposed scheme does not deteriorate the performance even if the secure communication is achieved by a pre-equalization mechanism.

Fig. 7 shows the bit error ratio performance of eavesdroppers in the proposed scheme. In this figure, eavesdroppers are assumed to exist at a different place of the receiver. Therefore, the channel state changes independently comparing to the channel state of the legitimate receiver. It means that the pre-equalized signal is affected by the two channel states: the channel between the transmitter and the legitimate receiver and the channel between the transmitter and the eavesdropper. Additionally, eavesdroppers cannot demodulate the signal correctly because they cannot obtain the channel state of the legitimate receiver. As a result, they suffer from bit errors due to failure of the demodulation. The results show that the bit error ratio performance is almost 0.5 in every channel model. Then, the decoded signals do not carry any information due to bit errors. This means that eavesdroppers cannot obtain any information from the pre-equalized signal, and the proposed scheme can realize secure communication by the pre-equalization mechanism.

### IV. Conclusion

This paper has proposed a new physical secure communication scheme by a pre-equalization mechanism. The proposed scheme has focused on difference of a channel state, and has utilized it as an encryption key for secure communication. A proposed transmitter estimates a channel state to a receiver, and pre-equalizes a signal before a packet transmission. Then, it also pre-equalizes the signal adapting for the receiver. Therefore, only legitimate receiver can obtain the undistorted
signal by passing the channel, and the other receivers receiver only the distorted signal due to the different channel state. As a result, the proposed scheme can realize a secure communication by using a channel state as an encryption key. The numerical results demonstrate that the legitimate receiver can realize a similar performance of the conventional IEEE 802.11a system and eavesdroppers cannot obtain any information from the signal due to erroneous data. The proposed scheme is a new type of secure communication depending on a channel state with conventional consumer devices, and will be a fundamental idea for a new approach.

**TABLE I**

<table>
<thead>
<tr>
<th>Model</th>
<th>Relative Delay [ns]</th>
<th>Average Power [dB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indoor residential A</td>
<td>0 50 100</td>
<td>-9.4 -18.9</td>
</tr>
<tr>
<td>Indoor office A</td>
<td>0 50 100</td>
<td>-3.6 -7.2</td>
</tr>
<tr>
<td>Indoor commercial A</td>
<td>0 50 100 150 200</td>
<td>-2.9 -5.8 -8.7 -11.6</td>
</tr>
<tr>
<td>Outdoor urban low-rise areas</td>
<td>0 50 150 325 550 700</td>
<td>-1.6 -4.7 -10.1 -17.1 -21.7</td>
</tr>
<tr>
<td>Low antenna A</td>
<td>0 50 100 150 200 250 300 350</td>
<td>-2.9 -5.8 -8.7 -11.6 -14.5 -17.4 -20.3</td>
</tr>
</tbody>
</table>

**TABLE II**

<table>
<thead>
<tr>
<th>Simulator</th>
<th>Matlab 2015b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of trials</td>
<td>10000</td>
</tr>
<tr>
<td>Communication device</td>
<td>IEEE802.11a</td>
</tr>
<tr>
<td>Number of symbols in a frame</td>
<td>10</td>
</tr>
<tr>
<td>Modulation scheme</td>
<td>QPSK</td>
</tr>
<tr>
<td>Number of FFT points</td>
<td>64</td>
</tr>
<tr>
<td>Number of data sub-carriers</td>
<td>48</td>
</tr>
<tr>
<td>Number of pilot subcarriers</td>
<td>4</td>
</tr>
<tr>
<td>Number of zero padding</td>
<td>12</td>
</tr>
<tr>
<td>Guard Interval</td>
<td>16 (0.8 [$\mu$s])</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>20 [MHz]</td>
</tr>
<tr>
<td>Frequency</td>
<td>5.2 [GHz]</td>
</tr>
<tr>
<td>Channel model</td>
<td>JTC Indoor commercial A</td>
</tr>
<tr>
<td></td>
<td>JTC Indoor office A</td>
</tr>
<tr>
<td></td>
<td>JTC Indoor commercial A</td>
</tr>
<tr>
<td></td>
<td>Outdoor urban low-rise areas</td>
</tr>
<tr>
<td></td>
<td>Low antenna A</td>
</tr>
<tr>
<td></td>
<td>Outdoor residential areas</td>
</tr>
<tr>
<td></td>
<td>Low antenna A</td>
</tr>
<tr>
<td></td>
<td>Rayleigh fading (Multi-path: 4)</td>
</tr>
<tr>
<td>Speed</td>
<td>1 [km/h]</td>
</tr>
</tbody>
</table>

**ACKNOWLEDGMENT**

This work is supported in part by Grant-in-Aid for Scientific Research (B)(15H02697) and Grant-in-Aid for Scientific Research (C)(26330103), Japan Society for the Promotion of Science (JSPS) and the Integration research for agriculture and interdisciplinary fields, Ministry of Agriculture, Forestry and Fisheries, Japan.
REFERENCES