A Study on a Transmit Antenna Directivity Control of Adaptive Array for Secure Wireless Transmission Based on the Multi-Path Routing

Masaaki YAMANAKA, Norihiko MORINAGA
Department of Information and Communication Technology
Hiroshima International University
Hirokoshingai 5-1-1, Kure, Hiroshima 737-0112, Japan
Email:{m-yamana, morinaga}@it.hirokoku-u.ac.jp

Shinichi MIYAMOTO, Seiichi SAMPEI
Graduate School of Engineering
Osaka University
Yamada-oka 2-1, Suita, Osaka 565-0871, Japan
Email: {miyamoto, sampei}@comm.eng.osaka-u.ac.jp

***Abstract*—This paper proposes an antenna directivity control method of adaptive array antenna for secure wireless transmission by dividing the transmitted information into pieces of divided-information and sending each pieces of information in a spatially distributed manner along multiple paths in a wireless space. Based on the DCMP weight control algorithm, the authors propose an antenna directivity control method not only to steer its main lobe to one targeted path but also to suppress other side lobes to suppress unnecessary signal radiation. Computer simulation confirms that by suppressing the side lobes of the antenna directivity, the transmitted signal power can be concentrated along the targeted path. It is effective to provide multiple transmission routes for signal delivery in the wireless space. Therefore better performance in regard with the secrecy of the transmitted information can be achieved in the wireless space by sending the transmitted information in a spatially distributed manner along the selected paths between the sender and the destination.**

I. INTRODUCTION

For safe and secure development of private wireless communication network it is mandatory to provide a high secured link-creation mechanism between terminals. Because nowadays, people can construct their own private wireless networks in various environments, e.g., train terminals, hotel lobbies, restaurants, and even in-transit time, etc., sent messages can be easily overheard by unintended listeners of the sender.

Multi-path routing [1]-[3] gathers a good attention to strengthen the confidentiality of the transmitted information. The notion of this method is to divide the transmitted information into some pieces of divided-information in advance and to send each pieces of information separately through different transmission routes to the destination. Because, by carefully selecting physically separated routes to the destination, the adversary cannot obtain all the necessary information to reconstruct the original information at the same time in the same location, it can strengthen the confidentiality of the original information from the information theory stand point of view.

Based on the idea of the multi-path routing, the authors have proposed a secure wireless link creation scheme in a wireless space by providing the multiple transmission routes around the multiple paths of the wireless link which the link possesses naturally on its own [4]. In the proposed scheme, at first, a plural number of transmission routes are created around the selected paths with individually controlled antenna directivities. Then, a well known secret sharing method [5][6] is applied to divide the original information into the same number of pieces of information as the number of transmission routes. Because the secret sharing method can divide the original information in such a way that nothing about the original information can be reconstructed unless all the shared pieces of information are obtained, by sending each shared pieces of information spatially separated manner through different transmission routes to the destination, the original information reconstruction can be confined to a limited area where all the shared pieces of information have been transmitted.

Antenna directivity control plays an important role in the proposed method to provide spatially separated transmission routes between the sender and the destination. It should be properly controlled to concentrate the transmitted signal power individually along each paths to confine the signal transmitted area around each paths. Adaptive array antenna (AAA) is a good candidate to control the antenna directivity to concentrate the transmitted signal power to an intended direction by steering the main lobe adaptively in the wireless space. However the side lobes of the antenna directivity still allow unintended signal radiation, which will widen the signal transmitted area along the selected paths thus deteriorates the secrecy performance of the original information achieved by the multi-path routing.

In this paper, we will propose an antenna directivity control method of AAA for the multi-path routing by deeply suppressing the side lobes of the antenna directivity to further concentrate the transmitted signal power along the selected paths. In the proposed method, a directionally constrained minimization of power (DCMP) weight control algorithm [7] is employed to create sufficient antenna gain to the direction of the selected paths, whereas a wide range of antenna null is created to the other direction to suppress unintended signal radiation occurred by the side lobes. Computer simulation confirms that with the proposed method, the transmitted sig-

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

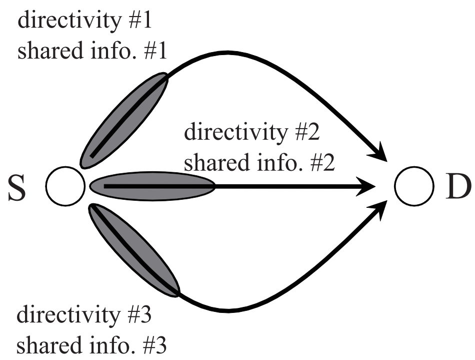

Fig. 1. A realization image of the proposed secure wireless transmission scheme

nal power is further concentrated along the selected paths, thus the spatial distributions of the transmission routes are arranged more along the selected paths. Therefore the better performance in regard with the secrecy of the transmitted information can be achieved by sending the information in a spatially distributed manner along the transmission routes between the sender and the destination.

The rest of the paper is arranged as follows. The overview of the secure wireless link creation scheme with the multi-path routing and the secret sharing method is described in sec. II. The proposed antenna directivity control method of AAA is introduced in sec. III. Then the effect of the side lobe suppressing of the proposed method is evaluated by computer simulation in sec. IV. Finally, a conclusion is made in sec. V.

II. Secure wireless link creation based on the multi-path routing and the secret sharing method

To review the mechanism of the information transmission from the information theory stand point of view, the original information cannot be reconstructed unless a necessary amount of information is delivered to the destination. The proposed scheme creates a secure wireless link based on this principle by combining the secret sharing method and the multipath routing.

The secret sharing method was proposed by Shamir in his original paper in 1979 [5]. He called the scheme (k, n) threshold scheme as it divides the original information into n pieces of shared information and only allows to reconstruct the original information when k shared pieces of information are obtained. Here each shared pieces of information is not a simple fragmentation of the original information, but a mathematical transformation such that each individual share does bear some information, but does not carry any meaningful portion of the original information. Even with infinite time and processing power, if the number of shares available is less than k, the adversary cannot get any meaningful information from the shares [6].

In our proposed scheme, at first, a plural number of propagation paths are selected to separately deliver the transmitted information to the target destination. Then, the transmitted information is divided into the same number of pieces of information as the number of the selected paths by the secret sharing method using the (n, n) threshold scheme. Here (n, n) threshold scheme divides the transmitted information into n pieces of shared information where the original information cannot be reconstructed unless all the n shared pieces of information are obtained. Therefore by sending the shared information individually through different selected paths, the original information reconstruction can be confined to a limited area where all the shared pieces of information have been transmitted. Fig. 1 shows one realization image of the secure wireless transmission scheme where three propagation paths are selected between the sender (S) and the destination (D). At first, at the sender, the transmitted information is divided into three pieces of shared information by $(3, 3)$ threshold scheme. Then each shared pieces of information are sent directing three different paths with individually controlled antenna directivities. It can be seen from Fig. 1 that a secure wireless link can be created between the sender and the destination because all the shared pieces of information cannot be obtained on the way to the destination at the same time in the same location.

In general, it is difficult to provide such spatially separated transmission routes in a wireless space even though directional antenna is employed at the sender. Because each paths are intricately overlapped and the transmitted signals spatially spread around the selected paths. However, although it cannot provide fully separated transmission routes to the destination, with directive transmission, the signal transmitted area of each shared pieces of information can be arranged to a limited area along each paths, i.e., the spatial distribution of the transmission routes can be arranged in different direction in the wireless space. This will confine the original information reconstruction because the (n, n) threshold scheme can restrain the original information recovery only when all the shared pieces of information are obtained.

Related work has been done in the paper [1]-[3]. In [1], the idea of the secret sharing method employed multipath routing is first applied in the wireless communication network, where the reliability of the transmitted information is discussed. In [2], the authors used the idea for the confidentiality of the transmitted information where a routing protocol of the multi-path routing is proposed. In [3], a directive transmission with directional antenna is examined for the multi-path routing where the confidentiality performance has been clarified by reducing the message interception probability in the network. However all these previous works assumed a multi-hop wireless network, i.e., separated routes of the multi-path routing are created by deploying proper intermediate relay terminals from the sender. Whereas in this paper, a single-hop wireless transmission is assumed, i.e., the separated routes are created using the multiple paths of the wireless link which the link possesses naturally on its own. To the best of the authors' knowledge, the notion of the multi-path routing is first applied to a single-hop wireless transmission environment where a secure transmission is discussed with the secret sharing method.

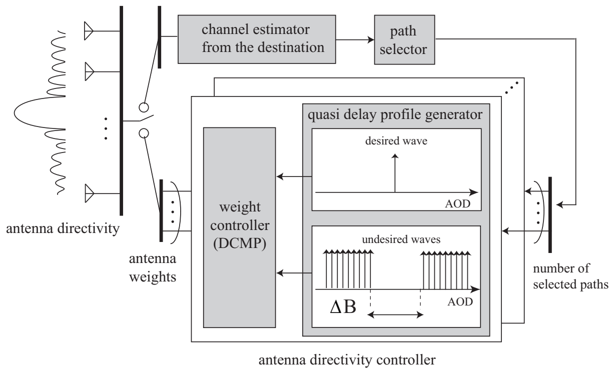

Fig. 2. Block diagram for creation of the antenna directivity

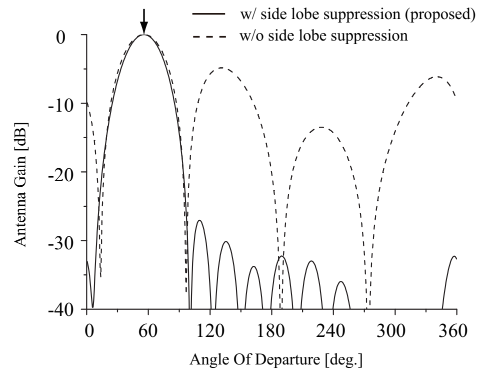

Fig. 3. Antenna directivity

III. Antenna Directivity Control Method

Transmit antenna directivity should be controlled properly to concentrate the transmitted signal power along each selected paths to form separated multiple transmission routes between the sender and the destination. AAA is a good candidate to control the antenna directivity to concentrate the signal power to an intended direction by steering the main lobe of the antenna directivity. However the side lobes still allow unintended signal radiation thus will widen the signal transmitted area along each selected paths.

In this section we will propose an antenna directivity control method of AAA based on the DCMP weight control algorithm not only to steer the main lobe to an intended direction but also to deeply suppress the side lobes to further concentrate the signal transmission power along each selected paths.

A. DCMP weight control algorithm

DCMP algorithm controls the antenna weights on the principle of minimizing the output power under the constrained response to specified directions [7]. The antenna weights ($\mathbf{W}$) are calculated by solving a conditioned power minimization problem indicated below [8], where $\mathbf{R}_{xx}$ is the correlation matrix among the array elements, $\mathbf{W}^*$ denotes complex conjugate of $\mathbf{W}$.

$$\overset{\mathbf{W}}{min}\left(P_{out}=\frac{1}{2}\mathbf{W}^H\mathbf{R}_{xx}\mathbf{W}\right) \tag{1}$$

$$\text{subject to } \ C\mathbf{W}^*=\mathbf{H} \tag{2}$$

Here Eq. (2) shows the directional constraint of the minimization problem, where C shows the constrained response and $\mathbf{H}$ shows the array response vector for the constrained direction. The Lagrange polynomial method can be applied to solve the above equation to derive the optimum antenna weights ($\mathbf{W}_{opt}$) indicated below.

$$\begin{aligned}\mathbf{W_{opt}} &= \gamma\mathbf{R}_{xx}^{-1}C\\ \text{where } \gamma &= \frac{\mathbf{H}^*}{C^*\mathbf{R}_{xx}^{-1}C}\end{aligned} \tag{3}$$

B. Antenna Directivity Control Procedure

In the proposed method, the angle of departures (AODs) of the selected paths are estimated and individually set as the constrained directions to derive the correspondent optimum antenna weight sets based on the DCMP algorithm. Moreover, a delay profile measurement based antenna weight control technique is employed to suppress unintended radiation to concentrate the transmitted signal power to the selected paths.

Fig. 2 shows the block diagram for creation of the antenna directivity. At first, at the “channel estimator” , a channel delay profile from the targeted destination is estimated. And at the “path selector”, a plural number of paths are selected and their angle of arrivals (AOAs) are estimated. In this paper, the spectrum is assumed to be shared by all terminals as in the case of the wireless LAN, therefore we assumed that the estimated AOAs of the selected paths are equal to the AODs of the same paths due to the channel reciprocity. Then at the “antenna directivity controller”, quasi delay profiles for transmission are created individually based on the AODs of the selected paths and the optimum antenna weights are derived based on the DCMP algorithm.

In each quasi delay profile, a desired wave is generated in the AOD of the selected path and a cluster of undesired waves are generated around the desired wave, where ΔB is the blank angle around the desired wave where the undesired waves are prohibited to generate. Here Eq. (2) indicates that the DCMP algorithm protects the output power for the constrained direction to be equal to the constrained response (C), therefore by setting the constrained direction as the AOD of the selected path and setting C relatively larger than the desired wave, a sufficient antenna gain can be created to the constrained direction. On the other hand by virtually generating undesired waves around the constrained direction, because the DCMP algorithm minimizes the output power under the constrained response, the antenna gain can be deeply suppressed around the constrained direction.

Fig. 3 shows one example of the antenna directivity of the proposed method where the AOD of the selected path is set as 55 deg. indicated by “↓” mark in the figure. In the evaluation, a circular array is assumed with 12 antenna elements and

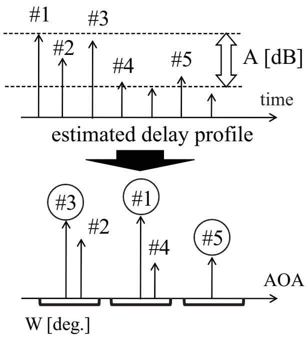

Fig. 4. Propagation path selection procedure

ΔB is set as 80 deg. For comparison, an antenna directivity formed by the minimum mean square error (MMSE) algorithm is also shown in the figure, where the antenna weights are controlled only to steer the main lobe to the AOD of the selected path, which we will use as a comparative method against our proposal throughout in this paper. From Fig. 3, we can see that with the proposed method, the main lobe is properly steered to the selected path direction, whereas the side lobes are deeply suppressed about 30 dB against the main lobe. This is because of the DCMP algorithm characteristic that it protects the constrained response under totally minimizing the output power.

C. Propagation path selection procedure

At the path selector, the sender should select appropriate paths to create separated transmission routes to the destination. We introduced two conditions for selecting appropriate paths to create spatially separated routes to the destination.

- Angle condition: If the AODs of the selected paths are nearly the same, they cannot provide spatially separated transmission routes to the destination. We introduced a condition that the AODs of the selected paths should be separated more than a certain angle (W).
- Power condition: If the propagation gain of the selected paths is not enough, the sender should increase its transmission power to successfully deliver the transmitted information to the destination. This will widen the signal transmitted areas around the selected paths and will make it difficult to provide spatially separated transmission routes to the destination. We introduced a condition that the propagation gain of the selected paths should be more than a certain level (A).

Fig. 4 shows one example of the selection of the propagation paths. It indicates that five paths ($\sharp$ 1 - $\sharp$ 5) which fulfill the power condition are selected as the candidate paths, then three paths ($\sharp$ 1, $\sharp$ 3, $\sharp$ 5) are selected from the candidate paths which fulfill the angle condition.

IV. Computer Simulation

The effect of the side lobe suppressing of the proposed method is evaluated in the IEEE802.11a wireless network

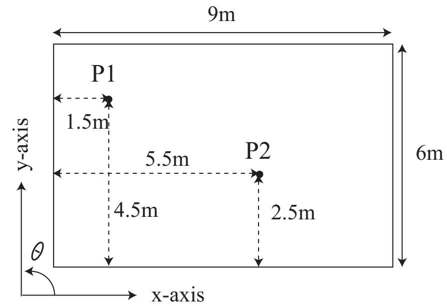

Fig. 5. Propagation environment

TABLE I
Simulation parameters

wireless transmission scheme	IEEE802.11a
array configuration	circular array
number of antenna elements	12
target received level at destination	-82 dBm
system sensibility level	-85 dBm
power condition (A)	30 dB
angle condition (W)	60 deg.

[9]. In this evaluation, we defined a metric "information transmission area" as the area where the information can be decoded in the physical layer that is the area where the transmitted signal can be observed higher than the system sensibility level. Because the metric indicates the area where the adversary can also decode and access the transmitted signal in the physical layer, we can use this metric to evaluate the security performance in the network from the physical layer security point of view.

A. Propagation model & Simulation parameters

Fig. 5 shows the propagation model used in the computer simulation. A wireless link from P1 to P2 is considered as indicated in the Fig. 5, where the propagation characteristic of the link is modeled by the ray-tracing method with up to two times of reflections.

Table I shows the simulation parameters used in the simulation. We assumed the IEEE 802.11a transmission scheme where the transmission power control is employed at the sender (P1) to control the received power level at the destination (P2) as -82 dBm which is the minimum received level defined in the IEEE 802.11a. The system sensibility level is set as -85 dBm which is 3 dB lower than the target received level at P2 assumed in this simulation.

B. Information transmission area of shared information

Based on the power condition and the angle condition listed on the Table I, the selected paths between P1 - P2 are determined. Table II shows the propagation gain and the AOD of the selected paths, where the propagation gain is normalized by the direct path (path $\sharp$ 1), and the AOD is defined as a horizontal angle from the X-axis specified in Fig. 5.

Because 6 paths are selected in this simulation. The original information is divided into 6 shared pieces of information

TABLE II
AOD AND ATTENUATION LEVEL OF THE PROPAGATION PATHS

path number	1	2	3	4	5	6
gain (dB)	0	-9.4	-11.1	-11.3	-17.6	-19.2
AOD (θ) (deg.)	330.3	55.0	299.1	197.1	227.1	23.5

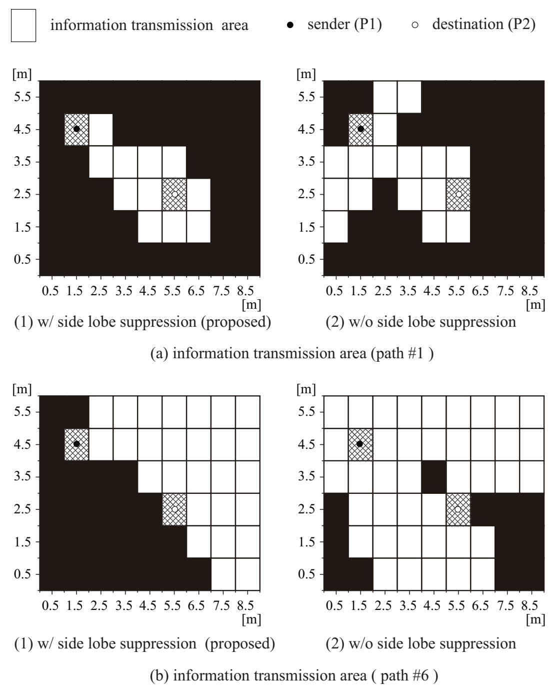

Fig. 6. Information transmission area of the shared information

and sent separately along 6 different paths to the destination. Fig. 6 shows the information transmission area of the shared information where (a) transmitted with ♯ 1 path, (b) transmitted with ♯ 6 path respectively. For comparison the performance without the side lobe suppressing is also shown in the figure. We can see form Fig. 6 that with the proposed method the information transmission area of the shared information can be confined along each selected path, i.e., the area is only distributed to the direction of the AOD of the selected path from the sender that is 330.3 degrees in figure (a), 23.5 degrees in figure (b) respectively.

C. Information transmission area of original information

The information transmission area of the original information can be derived as the area where all the shared pieces of information are obtained. Fig. 7 shows the information transmission area of the original information. For comparison the performance without the side lobe suppressing is also shown in the figure.

We can see from Fig. 7 that with the proposed scheme, the information transmission area of the original information has shrunk around the sender and the destination, i.e., the transmitted information is less exposed to the adversary in the wireless space. This is because the information transmission area of each shared pieces of information has arranged

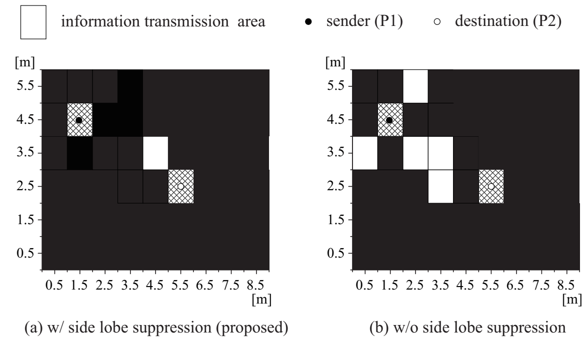

Fig. 7. Information transmission area of the original information

different direction along the selected paths, the multi-path routing works well with the secret sharing method to deliver the necessary information for reconstruction only to a limited area in the wireless space.

V. CONCLUSION

This paper proposed an antenna directivity control method for the multi-path routing in a single-hop wireless communication environment where multiple transmission routes are provided around the multiple paths of the wireless link which the link possesses naturally on its own. The authors employed DCMP weight control algorithm to deeply suppress side lobes of the antenna directivity to concentrate the transmitted signal power along specified paths selected in the wireless space.

With computer simulation, it is clarified that the proposed antenna directivity control method is effective to arrange the information transmission area of each shared pieces of information into different direction in the wireless space. By sending the original information in a spatially distributed manner with the multi-path routing and the secret sharing method, the original information reconstruction can be confined to a limited area around the sender and the destination, i.e., a secure wireless transmission can be achieved in the wireless space.

REFERENCES

[1] L. Zhou, Z. J. Hass, “Securing Ad Hoc Networks,” IEEE Network, Vol. 13, No. 6, pp. 24-30, Aug. 2002.
[2] W. Lou, Y. Fang, “A Multipath Approach for Secure Data Delivery, ” in Proc. of MILCOM 2001, Aug. 2001.
[3] V. Berman, B. Mukherjee, “Data Security in MANETs using Multipath Routing and Directional Transmission, ” in Proc. of ICC 2006, Jun. 2006.
[4] M. Yamanaka, S. Miyamoto, S. Sampei, N. Morinaga, “A Study on Secure Wireless Link Creation Based on Multi-Path Routing Combined with Transmit Antenna Directivity Control, ” in Proc. of INCoS 2011, Nov. 2011.
[5] A. Shamir, “How to share a secret,” Communications of the ACM, Vol. 22, No. 11, pp. 612-613, Nov. 1979.
[6] E. D. Karnin, J. W. Greene, M. E. Hellman, “On Secret Sharing Sysmtems, ” IEEE Tran. on Inform. Theory, Vol. IT-29, No. 1, Jan. 1983.
[7] O. Frost, “An Algorithm for Linearly Constrained Adaptive Array Processing,” Proceedings of the IEEE, Vol. 60, No. 8, Aug. 1972.
[8] K. Takao, M. Fujita, T. Nishi, “An Adaptive Antenna Array under Directional Constraint,” IEEE Trans. on Antenna and Propagation, Vol. AP-24, No. 5, pp. 662-669, Sept. 1976.
[9] IEEE Std 802.11-2007, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standards Association, 2007.