様式：課程博士用

2013年　9月　25日

電子・情報工学専攻	学籍番号	063414
申請者 氏名	坂井　尚貴	

指導 教員	大平 孝

論　文　要　旨　(博士)

論文題目	無線秘密鍵生成共有方式の秘匿性を高める可変指向性アンテナの研究

(要旨　1,200字程度)

本論文は無線秘密鍵生成共有方式の秘匿性を高める3素子ダイポールエスパアンテナとUSBメモリスティック型エスパアンテナの設計および試作について述べる．無線通信で送受する情報は暗号技術を用いる．暗号技術の1つに共通鍵暗号プリミティブがある．共通鍵暗号プリミティブは暗号と復号に共通の鍵を使うことが特徴である．共通鍵を盗聴局に盗まれること無く，安全に正規局で共有することが重要である．これを鍵配送問題という．無線秘密鍵生成共有方式は鍵配送問題を解決する技術である．本方式は電波の空間的ゆらぎと時間的ゆらぎから，鍵の生成と共有を行なう．電波のゆらぎは周辺の伝搬環境の変化，正規局に搭載された可変指向性アンテナの指向性パタンの変化で生成される．しかし，本方式が生成する鍵は周辺環境または可変指向性アンテナの性能次第では，配列が単調になり，一部が盗聴局に推定される．我々は鍵の秘匿性を高めるための手段として可変指向性アンテナの設計および試作する．鍵の秘匿性を高める可変指向性アンテナを設計試作するには，設計指標が必要である．

本論文は，無線秘密鍵生成共有方式で生成する鍵の秘匿性を向上させるアンテナ設計指標を提案，その有効性を明らかにする．アンテナ設計指標を用いて 3 素子エスパアンテナを設計および試作する．エスパアンテナは小型，小電力の特長をもつ可変指向性アンテナである．本方式は計算資源が少ない小型無線通信端末への応用が期待されおり，望まれるアンテナの特長は小型，小電力と，エスパアンテナの持つ特長と一致する．最後に3素子エスパアンテナの設計試作の成果を発展させUSBスティック型エスパアンテナを試作，評価する．電波のゆらぎと指向性の関係に着目し 5 つのアンテナ設計指標を提案する．アンテナ指標は，指向性パタンを評価する「指向性の複雑性評価指標」と，指向性パタン群を評価する「指向性の多様性評価指標」の 2 種類ある．複雑性評価指標として，エンドファイア・ブロードサイド比（EBR），軌跡長（LLL），累積ビーム幅（CBW）を提案する．多様性評価指標として，パラメータ領域指向性相関係数（PDC），指向性パタン相関係数（ADC）を提案する．受信信号対雑音電力比 0dB 以上，直接波対反射波電力比 3dB 以下の伝搬環境条件において，提案した指標の中でPDCと鍵の秘匿性指標（正規盗聴局間受信信号履歴相関係数）が最も高い正の相関性を示した．故にPDCの低減は鍵の秘匿性向上に有用である．次にPDCを用いて3素子ダイポールエスパアンテナの最適な素子間隔を解析と実験で探究する．結果，最小PDCが得られる素子間隔は1/16波長を示した．前述の結果を基に，USBメモリスティック型エスパアンテナを設計，試作した．素子間隔が1/4波長の3素子ダイポールエスパアンテナと比較し，試作したUSBスティック型エスパアンテナは，鍵の秘匿性指標Imacが0.01向上，サイズが1/8小型化を達成した．

year month day
2013 9 25

Department	Electronic and Information Engineering	ID	063414
Name	Naoki Sakai		

Supervisor	Takashi Ohira

Abstract

Title	Variable Beamforming Antennas for Wireless Secret Key Agreement Systems

(800 words)

This paper presents a three-element dipole ESPAR antenna and a USB stick ESPAR antenna for variable beamforming in wireless secret key agreement system. Wireless communication exchanges data in safety by cryptography technologies. The modern field of cryptography technologies is divided into two areas of symmetric-key cryptography and public-key cryptography. In the symmetric-key cryptography, a regular terminal needs to exchange a secret key with its party terminal for applying the secret key to encryption and decryption. This exchange must be done in secret from eavesdroppers. However, that is difficult in wireless communication systems. This is because, if the regular terminal transmits the key on a radio wave, it is easily intercepted by eavesdroppers. This is called key distribution problem. As a solution of this problem, a wireless secret key agreement system was proposed. The system generates and shares the key by making full use of wave fluctuations in space and time. The wave fluctuations are generated by changing the radio propagation environment around the terminals or varying the directivity of a variable beamforming antenna. However, the system has a problem. This problem is that a part of the key is estimated to intercept wave fluctuations by eavesdropper under some propagation property or antenna performance conditions. As degree of the key that isn't estimated by eavesdropper, secrecy of the key is defined. As a solution to achieve high secrecy of the key, we design and prototype variable beamforming antennas. This is because, secrecy of the key depends on wave fluctuations, and wave fluctuation is generated directivity fluctuation formed by the antenna. We expect to improve secrecy of the key when the antenna is designed by FoMs to indicate its performance. However, there are no FoMs that correlate with the secrecy of the key. Therefore, there is not a report on an antenna design and prototype for the system.

This paper aims to establish a variable beamforming antenna technology that improves the performance of wireless secret key agreement systems. We propose five FoMs for antenna directivity that correlate with the secrecy of the key to generate. The FoMs are defined from relation between the directivity and the wave fluctuations made by controlling the directivity. We show the validity of the proposed FoMs by computer simulation. This is done by showing the cross correlation coefficient between secrecy of the key and the FoMs. Based on the FoMs, we design and prototype two kinds of variable beamforming antennas.

First, we define five antenna FoMs. These FoMs are classified into two categories: (1) FoM of directivity complexity and (2) FoM of directivity diversity. The FoM of directivity complexity shows fluctuation quantity of directivity. As the FoM, Endfire to Broadside Ratio (EBR), Locus Line Length (LLL), and Cumulative Beam Width (CBW) are proposed. The FoM of directivity diversity shows directivity fluctuation independence of space and time. As the FoM, Parameter Domain Correlation coefficient (PDC) and Azimuth Domain Correlation coefficient (ADC) are proposed.

Next, we describe about the validity of the five FoMs. We investigate two characteristics by the system simulation. First characteristic is percentage of improving secrecy of the key by the FoMs. Second characteristic is a cross correlation coefficient between secrecy of the key and the

FoMs. RS profile correlation coefficient between regular terminals and an eavesdropper is defined as secrecy of the key. RS profile is values before quantizing the key. Simulation model of wave propagation is Transmit-Receive Beamlet Correspondence model. As results, validity of PDC is highest compared with other the FoMs. The cross correlation coefficient between PDC and secrecy of the key shows above 0.77 at RNR over -10 dB and K factor below 3 dB. And, the percentage of improving secrecy of the key gets up to 40¥%. RNR and K factor are wave propagation properties. RNR is Received signal to Noise Ratio. K factor is Direct wave to Reflection wave Ratio.

Then, we design and prototype variable beamforming antennas based on PDC. The system employs an ESPAR antenna. This is because, features of ESPAR antenna conforms with feature of a antenna desired by the system. The system is expected to apply mobile communication required very little computational resource. Therefore the system desires antenna features of compact size, low power consumption, and low cost. The ESPAR antenna has the same antenna features as ones. We investigate optimal element space of 3-element ESPAR antenna for the system by PDC in analysis and measurement of directivity. As the result, optimal element space is sixteenth-wavelength.

Finally, we prototype a USB stick ESPAR antenna by utilizing the previous results. The antenna shows downsizing of one-eighth and the slightly better value of PDC in comparison with the 3-element dipole ESPAR antenna having quarter-wavelength element space.