TOYOHASHI
UNIVERSITY OF TECHNOLOGY

エスパアンテナ秘密鍵生成システム秘匿性向上技術

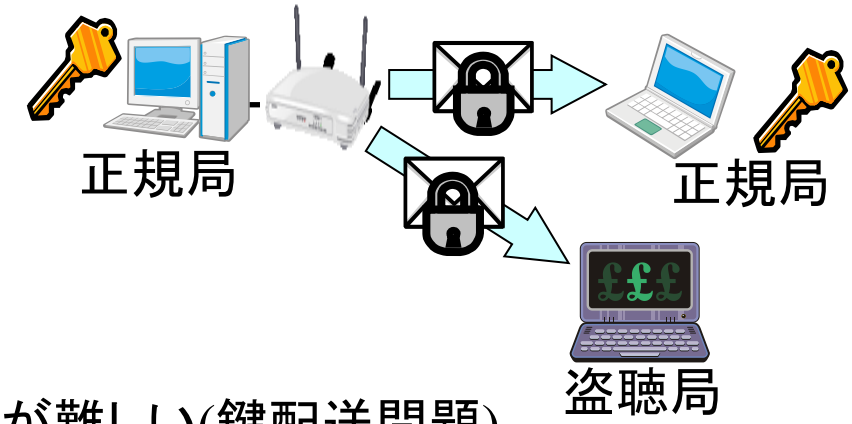
豊橋技術科学大学　大学院　工学研究科　電気・電子情報工学専攻
波動工学研究室　吉田斉史

合同修論発表会
平成25年2月1日(金)

1. 背景
2. エスパアンテナを用いた無線秘密鍵共有方式
3. 直接波が与える影響
4. 先行研究
5. 提案手法：固有値除去手法
6. シミュレーション
7. 実機実験
8. まとめ

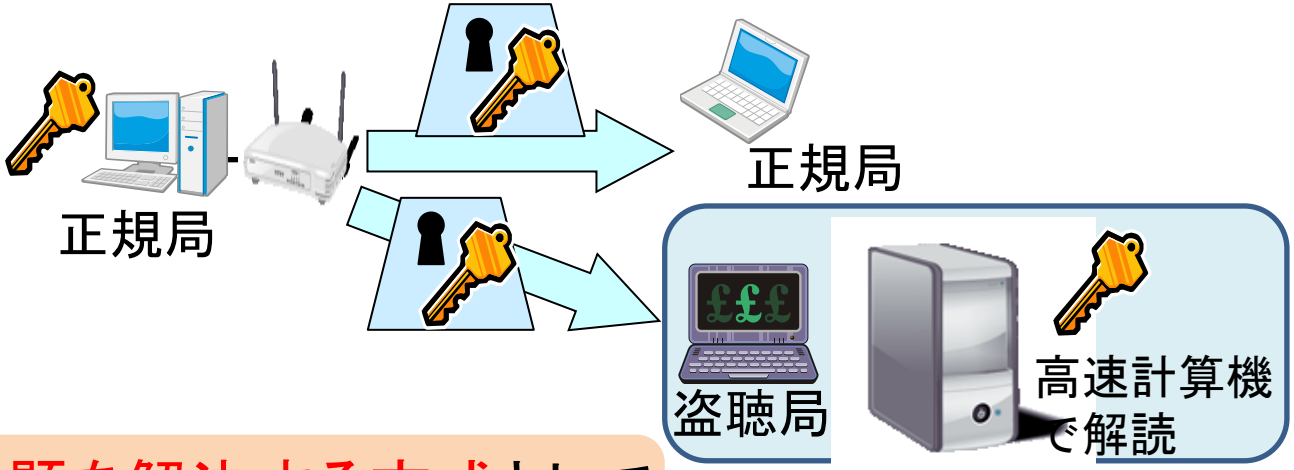
背景

無線通信では暗号化が必須



現在の暗号化方式には問題

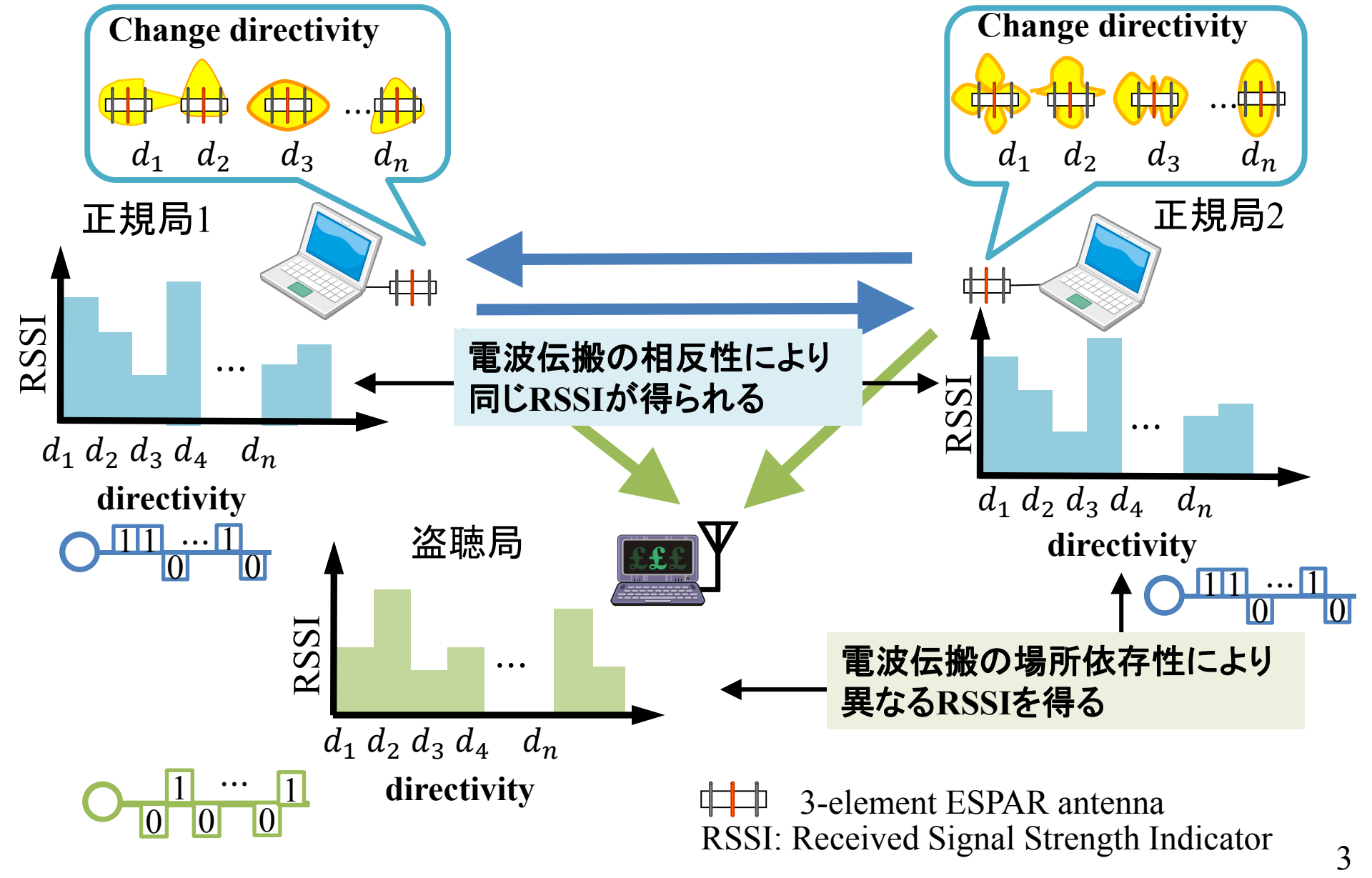
- 第三者に秘密裏に鍵を共有することが難しい(鍵配送問題)
- 将来的に公開鍵で暗号化された秘密鍵が解読される可能性がある



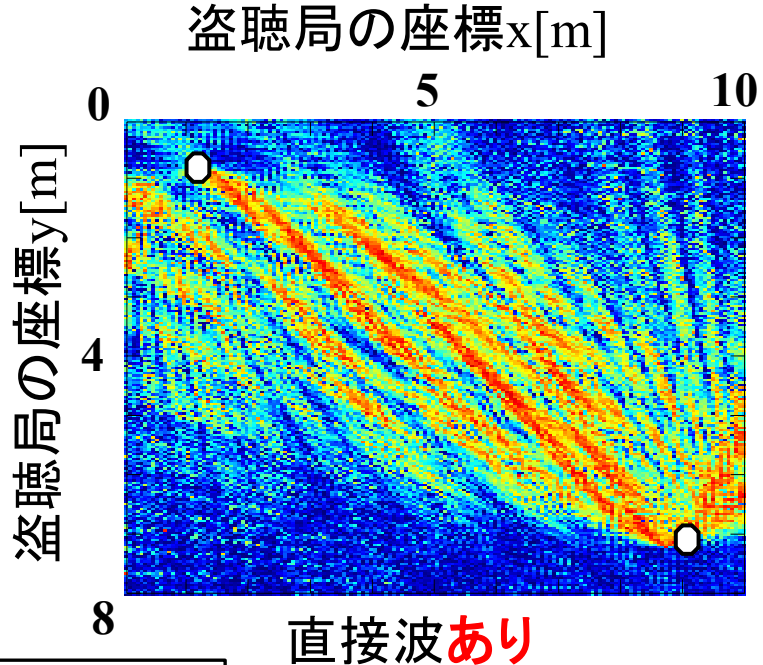
鍵配送問題を解決する方式として
エスパアンテナを用いた秘密鍵生成共有方式が提案[1]

[1] T. Aono, et al. “Wireless secretkey generation exploiting reactance-domain scalar response of multipath fading channels, ”IEEE Trans. Antennas Propag., vol.53, no.11, pp.3776-3748, Nov.2005.

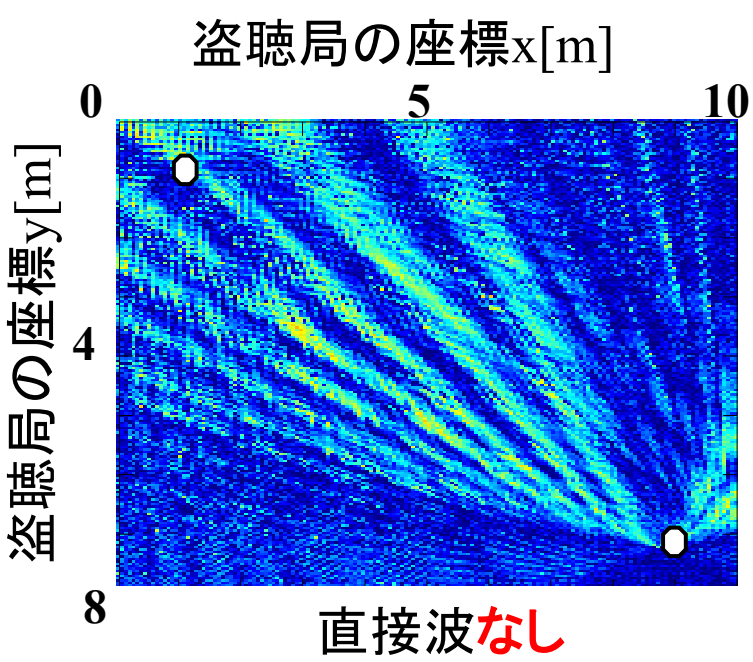
エスパアンテナを用いた無線秘密鍵生成共有方式



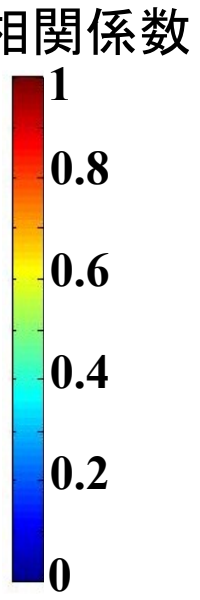
直接波が与える影響



直接波**あり**



直接波**なし**



○ 正規局

正規局と盗聴局のRSSIの相関係数

$$|\rho| = \frac{\left|\sum\left\{(x_i-\bar{x})(y_i-\bar{y})\right\}\right|}{\sqrt{\sum(x_i-\bar{x})^2}\sqrt{\sum(y_i-\bar{y})^2}}$$

x_i : i番目の正規局RSSI　y_i : i番目の盗聴局RSSI

$\bar{x}$:正規局RSSIの平均　$\bar{y}$:盗聴局RSSIの平均

直接波を除去するとRSSIの相関係数が低下

直接波を除去することで秘匿性が向上

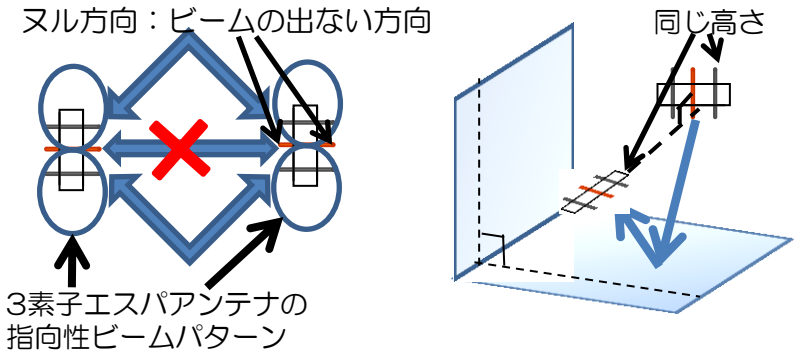
先行研究　直接波除去手法

□物理的な除去手法[2]

ヌル法：指向性のヌルを向け合う

偏波法：偏波の異なるアンテナを利用する

- **直接波を完全に除去できる**
- **直接波が除去され通信が行いにくくなる**
- **使用に制約が存在する**

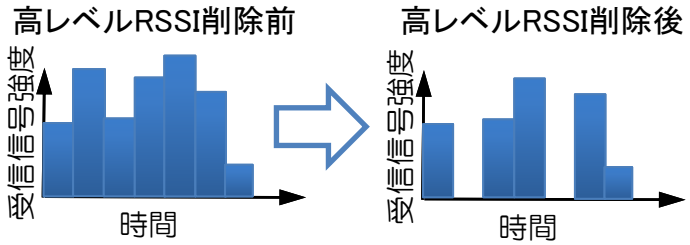


□ 信号処理による除去手法 [3]

高レベルRSSI削除

高レベルなRSSIは直接波成分が多く含まれている

- **直接波を完全に除去できない**
- **通信に影響を及ぼさない**
- **使用に制約が存在しない**



現在の状況

◇信号処理による手法の方が様々な環境に使用可能．しかし、報告が少ない．

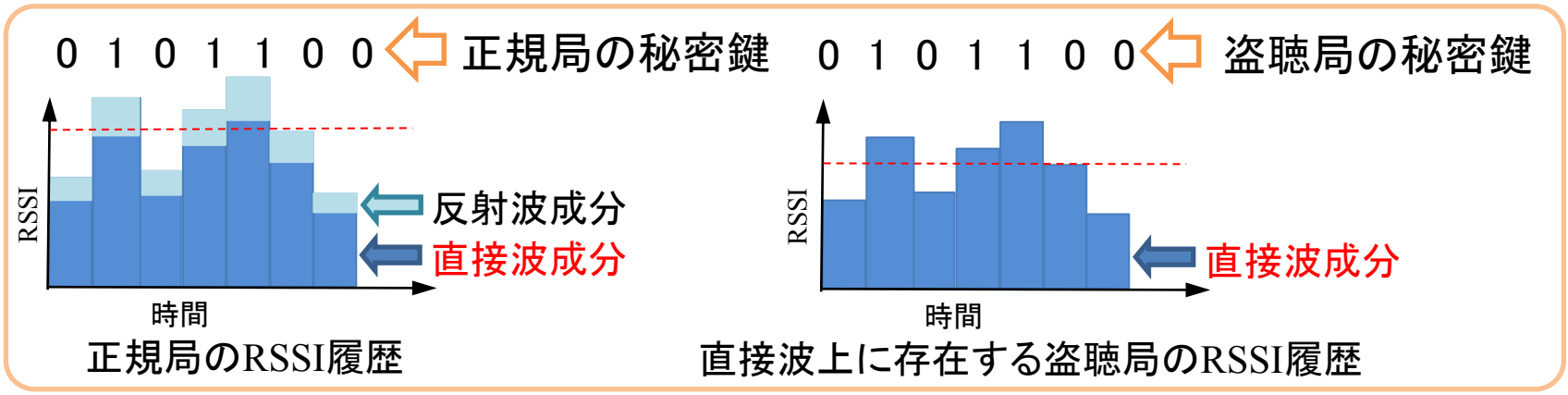
信号処理による秘匿性向上手法を新たに提案する

[2] 斎藤隆史,“両端末にエスパアンテナを用いた無線秘密鍵共有方式の安全性を向上する研究,”豊橋技術科学大学修士論文，Jan.2012.

[3] 清水崇之，岩井誠人，笹岡秀一,“エスパアンテナを用いた秘密鍵共有方式における盗聴耐性の高い鍵生成法,”信学論(B)，vol.92，no.9，pp.1348-1361，Sep.2009.

固有値除去手法の提案

□直接波が盗聴局に傍受されると



RSSI履歴に**支配的な影響を与える成分を傍受される**ことで**秘匿性が低下**

RSSI履歴に**支配的な影響を与える成分を除去する**ことで**秘匿性が向上**

信号処理により支配的な影響を与える成分を求める方法

固有値分解

第一固有値も支配的な影響を与える成分として考えられる

提案手法:固有値除去手法

□提案する手法

RSSIの変動に支配的な影響を与える成分を求め除去する(固有値分解を利用)

2つのオプションを提案

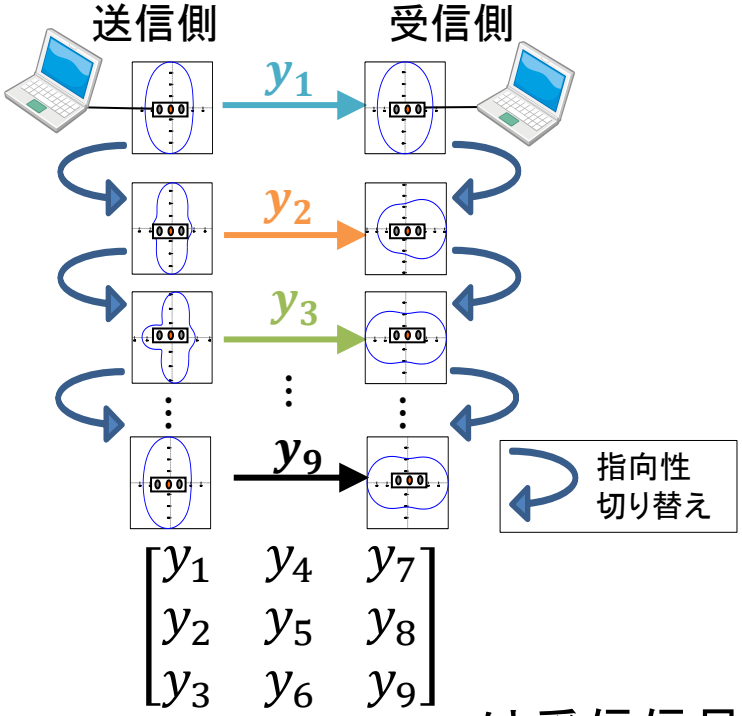
今回報告する内容

・オプション1:指向性の切り替えタイミングが送受で異なる

・オプション2:指向性の切り替えタイミングが送受で同じである

□オプション2による固有値計算方法

□手順1:行列生成



$$\begin{bmatrix} y_1 & y_4 & y_7 \\ y_2 & y_5 & y_8 \\ y_3 & y_6 & y_9 \end{bmatrix}$$

□手順2:固有値分解

$$\begin{bmatrix} y_1 & y_4 & y_7 \\ y_2 & y_5 & y_8 \\ y_3 & y_6 & y_9 \end{bmatrix} = P \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} P^{-1}$$

P:固有ベクトルからなる行列

λ:固有値

□手順3:固有を除去し，再計算

(第一固有値を除去する場合)

$$P \begin{bmatrix} 0 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} P^{-1} = \begin{bmatrix} y'_{11} & y'_{12} & y'_{13} \\ y'_{21} & y'_{22} & y'_{23} \\ y'_{31} & y'_{32} & y'_{33} \end{bmatrix}$$

yは受信信号振幅

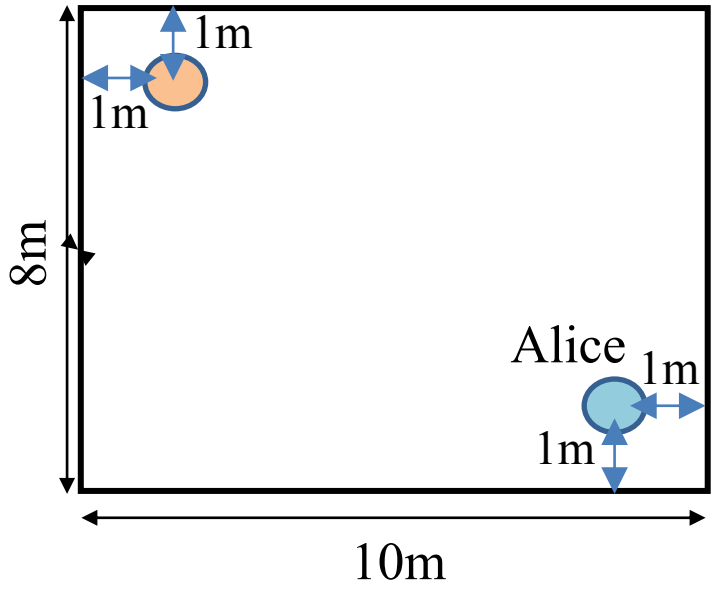
シミュレーション概要

手法の評価に必要なシミュレーション

雑音のない環境下で秘匿性を評価

雑音のある環境下で秘匿性を評価

相関係数で評価



反射パスモデル	2次元レイトレース
反射回数	6回反射まで
部屋サイズ	10m×8m
壁の材質	コンクリート
正規局アンテナ	3素子エスパアンテナ
正規局位置	(1,1),(9,7)
正規局の指向性	ランダム
盗聴局アンテナ	無指向性アンテナ
盗聴局位置	5cm間隔で配置
一箇所での鍵長	512bits

雑音のない環境下での評価指標
正規局と盗聴局のRSSIの相関係数

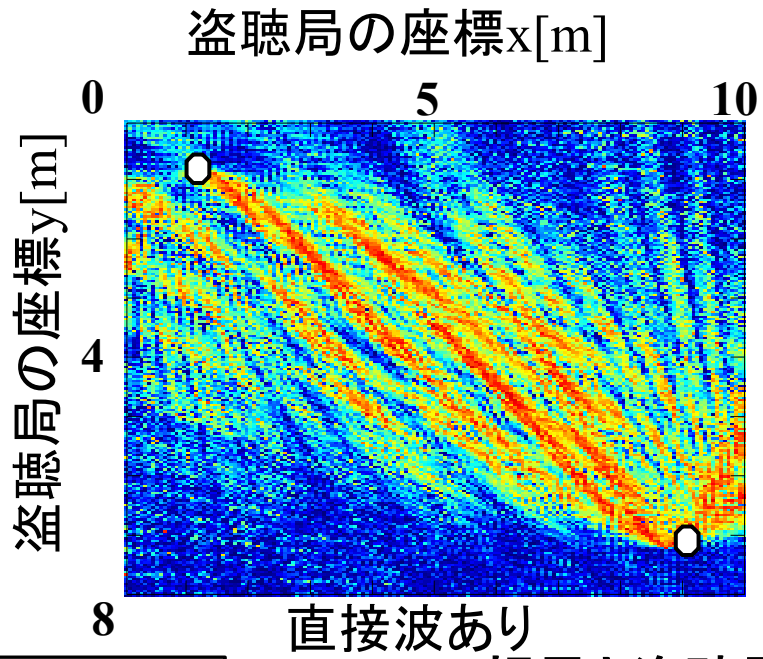
$$|\rho| = \frac{\left|\sum\left\{(x_i-\bar{x})(y_i-\bar{y})\right\}\right|}{\sqrt{\sum(x_i-\bar{x})^2}\sqrt{\sum(y_i-\bar{y})^2}}$$

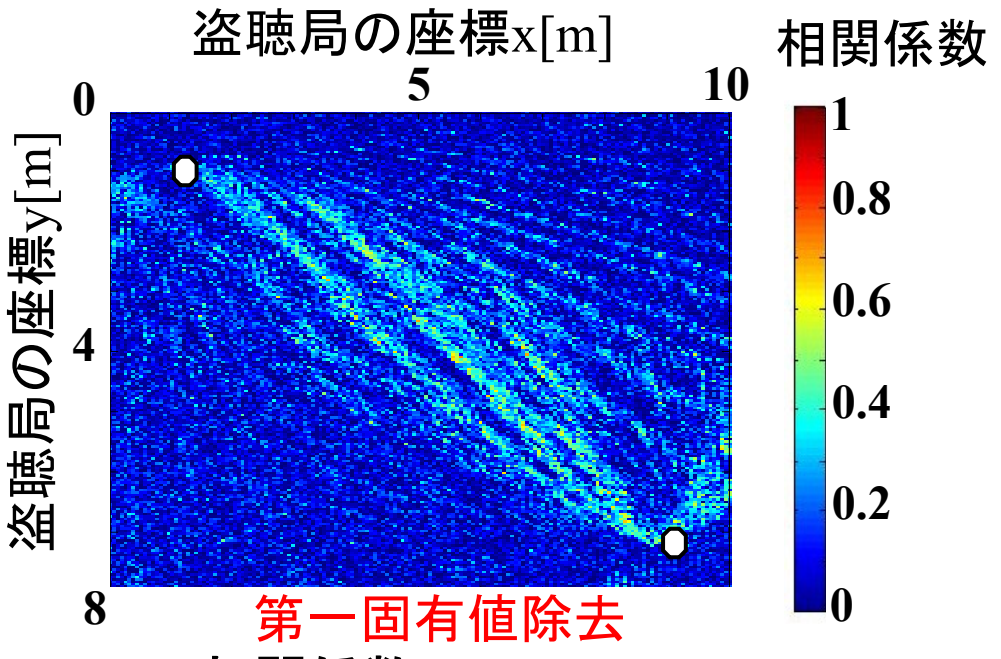
x_i : i番目の正規局RSSI　y_i : i番目の盗聴局RSSI

$\bar{x}$:正規局RSSIの平均　$\bar{y}$:盗聴局RSSIの平均

TOYOHASHI UNIVERSITY OF TECHNOLOGY

雑音のない環境下でのシミュレーション結果





○ 正規局

正規局と盗聴局のRSSIの相関係数

$$|\rho| = \frac{\left|\sum\left\{(x_i-\bar{x})(y_i-\bar{y})\right\}\right|}{\sqrt{\sum(x_i-\bar{x})^2}\sqrt{\sum(y_i-\bar{y})^2}}$$

x_i : i番目の正規局RSSI　y_i : i番目の盗聴局RSSI

$\bar{x}$:正規局RSSIの平均　$\bar{y}$:盗聴局RSSIの平均

第一固有値除去により**秘匿性の向上を確認**

シミュレーション概要

手法の評価に必要なシミュレーション

雑音のない環境下で秘匿性を評価

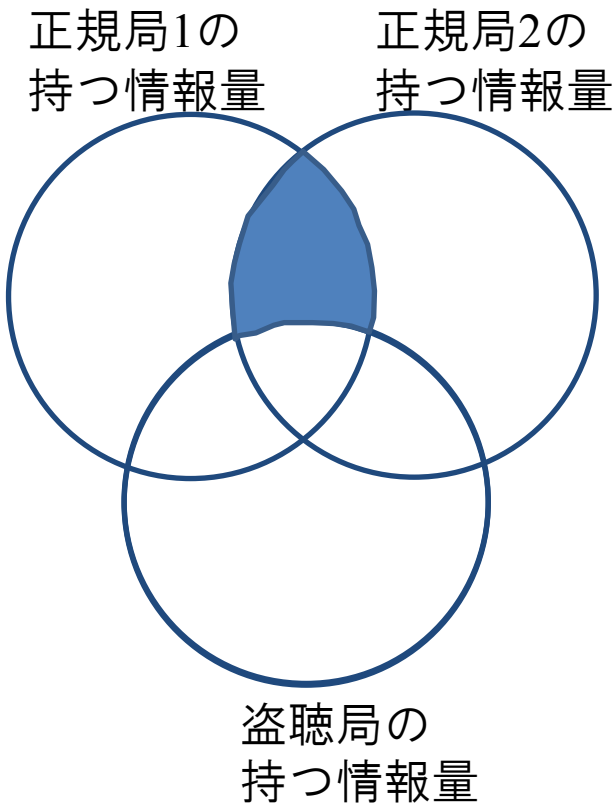
雑音のある環境下で秘匿性を評価

情報量(Imac)で評価

Imac(Information on mutual anti-tapping condition)
秘匿条件付き相互情報量[4]
正規局間でのみ共有した情報量

I_{mac}=H(正規局1|盗聴局)-H(正規局1|盗聴局,盗聴局)

Hは情報エントロピーを求める関数



鍵1bitの組み合わせと発生確率

発生確率	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
正規局1	0	0	0	1	0	1	1	1
正規局2	0	0	1	0	1	0	1	1
盗聴局	0	1	0	0	1	1	0	1

[4]長谷川拓ら,.“両端末に3素子エスパアンテナを用いた秘密鍵共有システムにおける秘匿条件付き相互情報量,”信学技報, vol.108, no.61, pp.13-18, May.2008.

シミュレーション概要

手法の評価に必要なシミュレーション

雑音のない環境下で秘匿性を評価

雑音のある環境下で秘匿性を評価

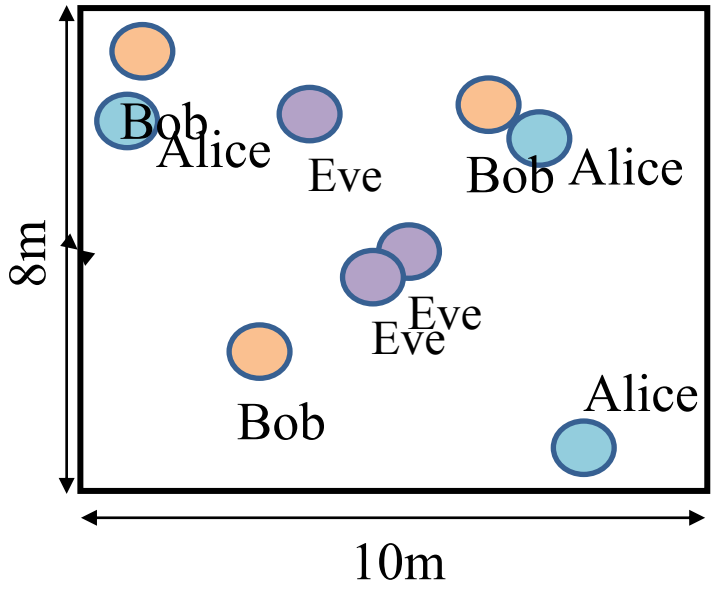
情報量(Imac)で評価

雑音は複素ガウス雑音で与える

$$\sqrt{P_n/2}(a+jb)$$

P_n:雑音電力

a, b:平均0,分散1の正規分布に従う乱数

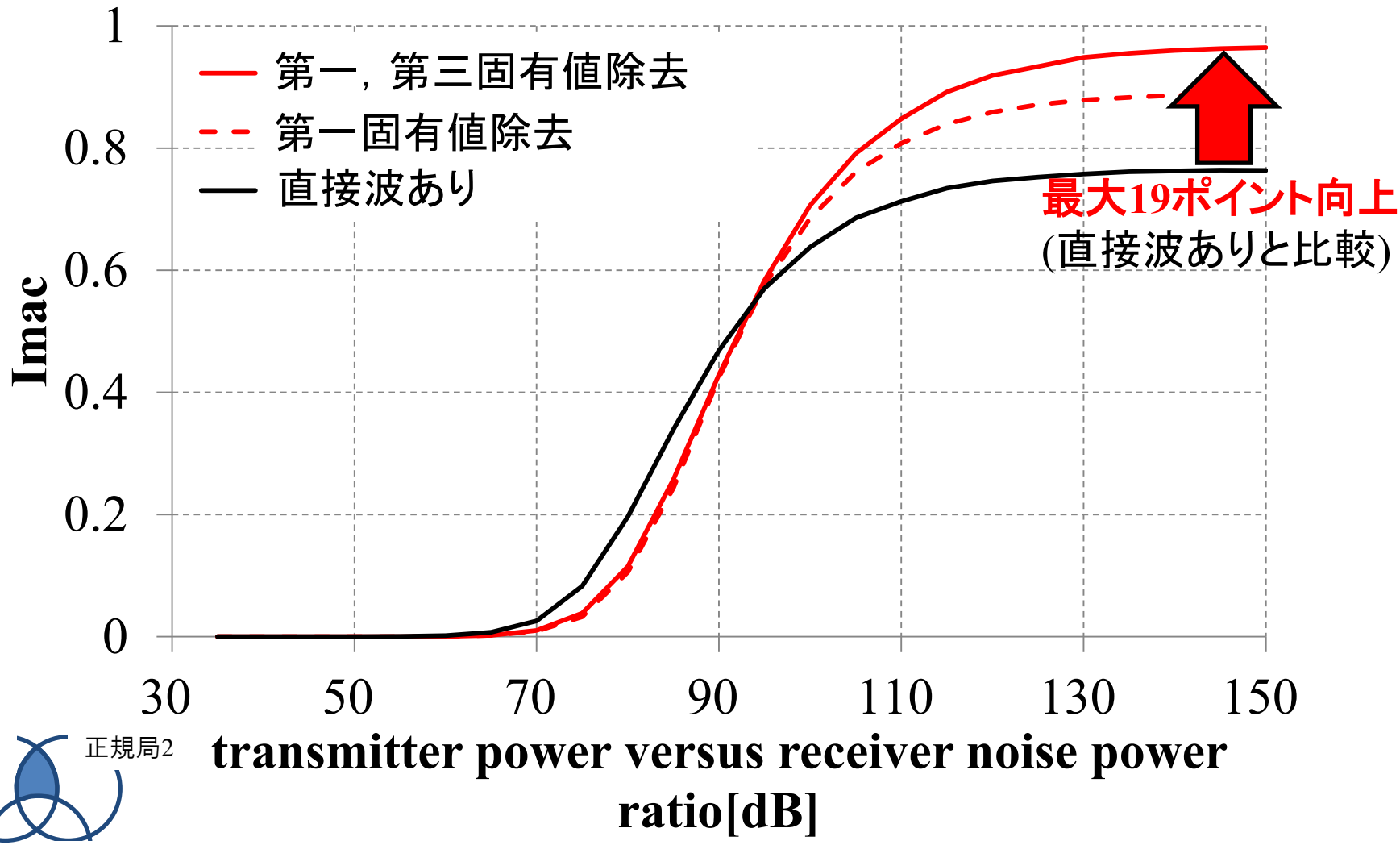


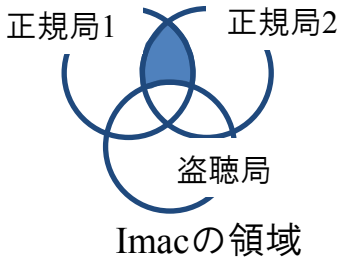
反射パスモデル	2次元レイトレース
反射回数	3回反射まで
部屋サイズ	10m×8m
壁の材質	Concrete
正規局アンテナ	3素子エスパアンテナ
正規局位置	ランダム
正規局の指向性	ランダム
盗聴局アンテナ	無指向性アンテナ
盗聴局位置	正規局の中点
全鍵長	216000 bits
位置変化回数	30回
一箇所での鍵長	216000/30 bits

216000bitsの鍵でImacを算出

Imac(正規局間でのみ共有した情報量)

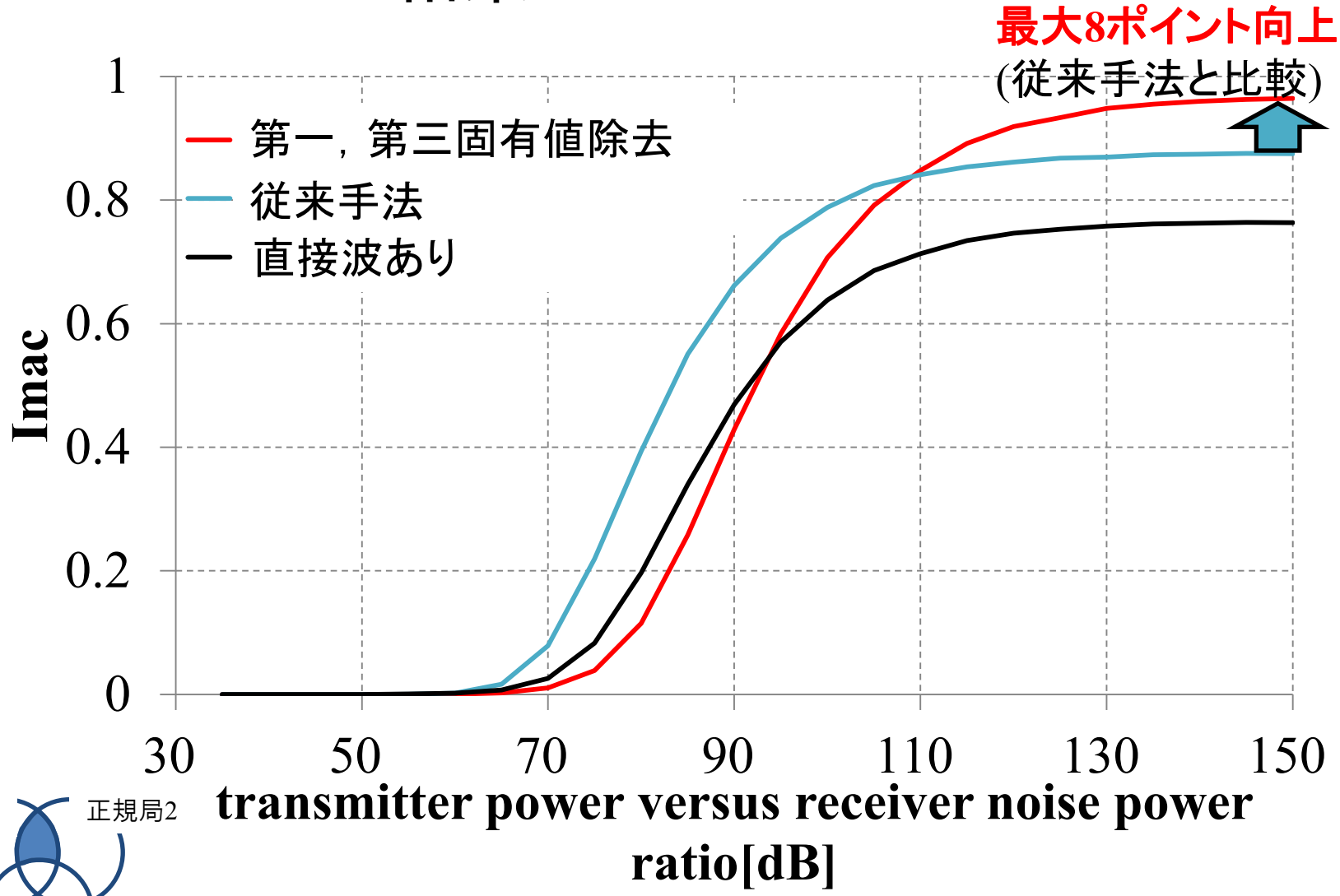
シミュレーション結果

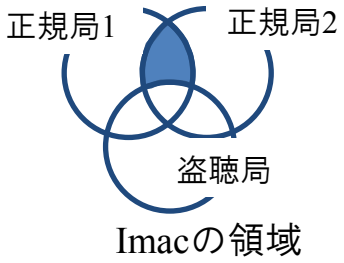




提案手法によるImac向上を確認

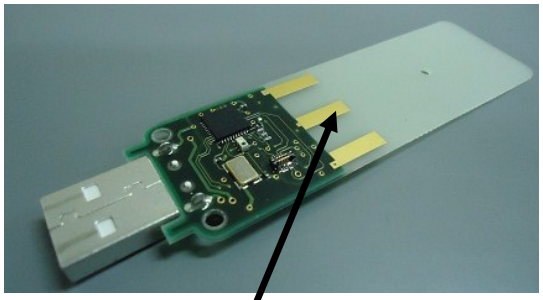
シミュレーション結果





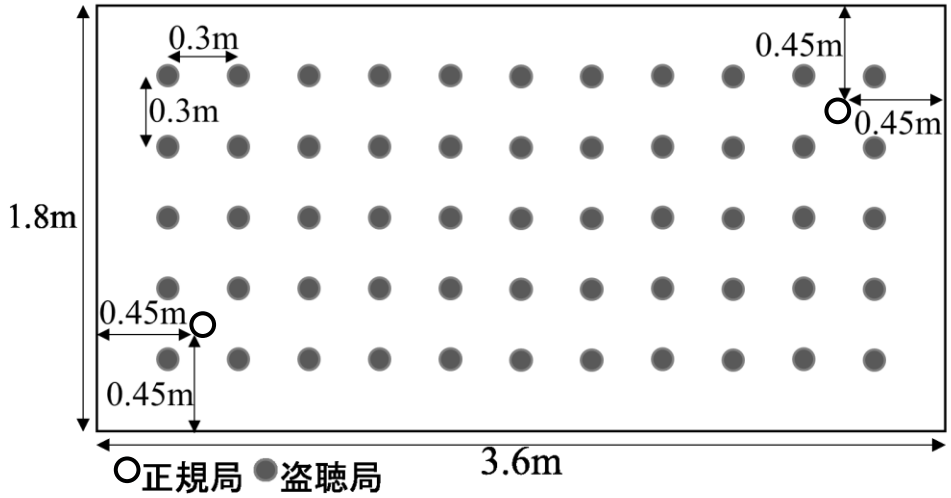
従来手法よりImacが向上することを確認

実機実験諸元

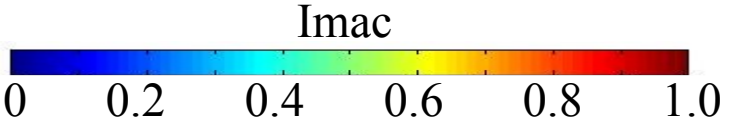


給電素子
USB型3素子エスパアンテナ

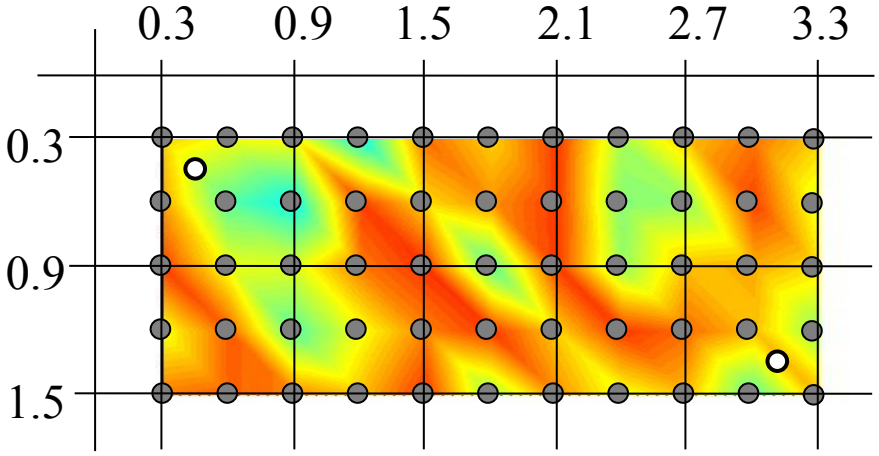
部屋サイズ	1.8m×3.6m×1.3m(高さ)
壁の材質	アルミシート
正規局の位置	(0.45,0,45),(3.15,1.35)
盗聴局の位置	55点
鍵長	511bits
正規局アンテナ (ZigBee規格)	USB型3素子エスパアンテナ
盗聴局アンテナ (ZigBee規格)	USB型3素子エスパアンテナ (無指向性で固定)
TNR	115.4dB



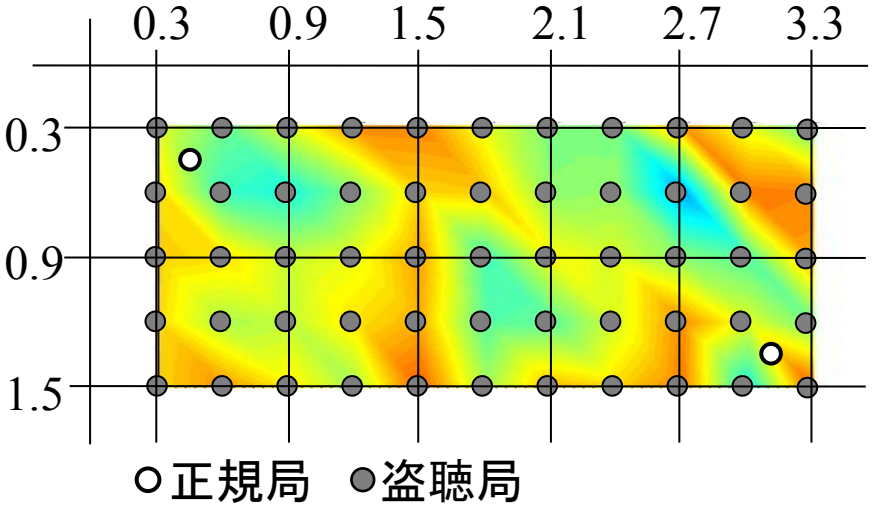
Imacの分布

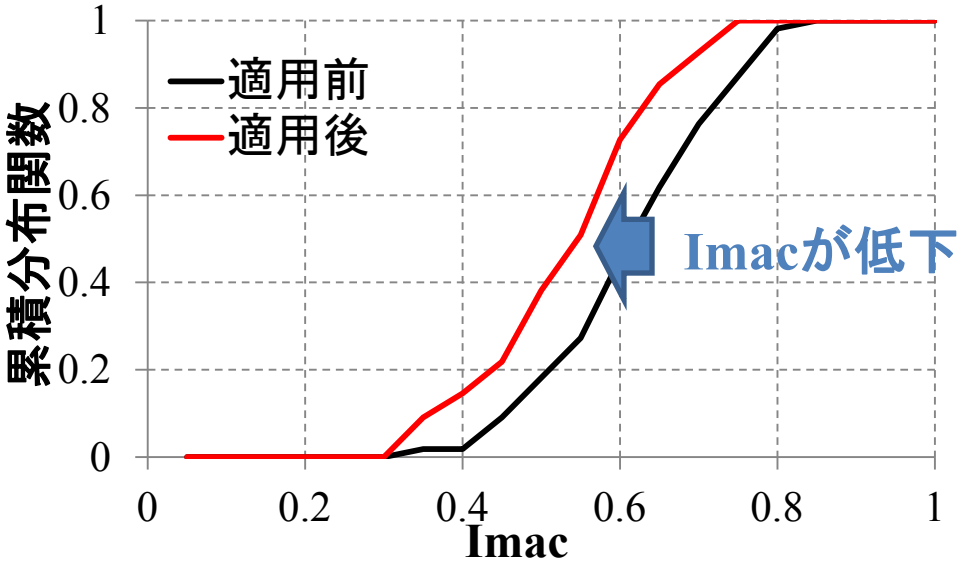


提案手法適用前



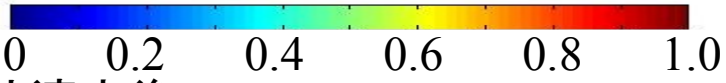
提案手法適用後



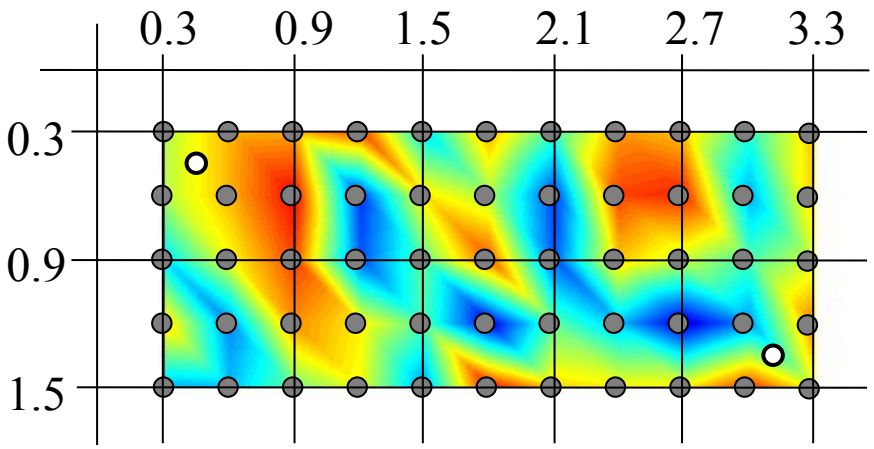


提案手法の適用により
Imacの低下を確認

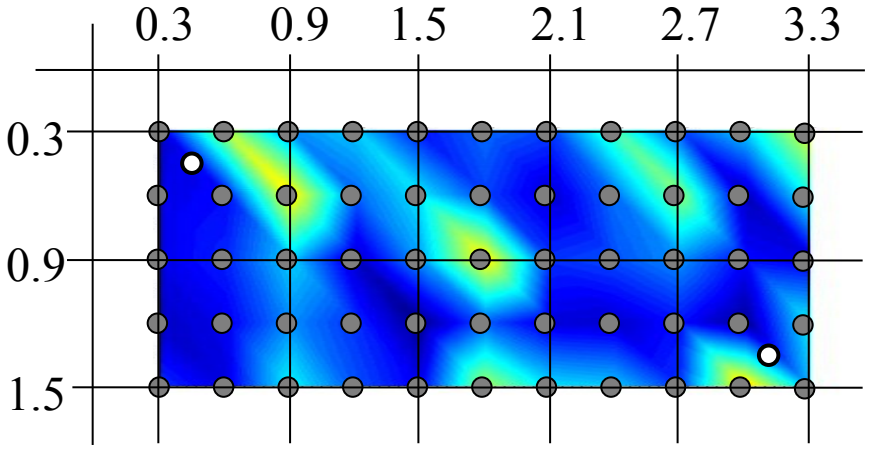
正規局-盗聴局間のRSSI相関係数



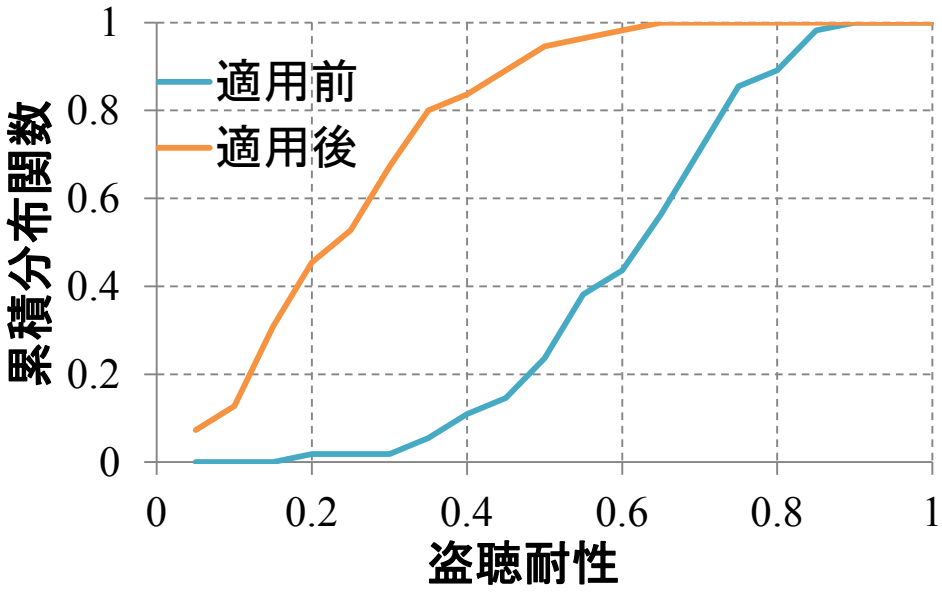
提案手法適用前



提案手法適応後



○正規局　●盗聴局



直接波上の相関がもともと低く
直接波の影響が少ない.

直接波の影響が少ない環境では
手法の適用によりImacが低下する
可能性がある

まとめ

シミュレーション結果まとめ

・秘匿性を向上させる信号処理手法を提案

・直接波ありと比較して
　Imac最大19ポイント向上を確認

・高レベルRSSI削除と比較して
　Imac最大8ポイント向上を確認

実機実験結果まとめ

・USB型3素子エスパアンテナを用いて
　提案手法の実機実験を行った

・提案手法による**秘匿性向上を確認できなかった**