無線物理層セキュリティを用いたIoTネットワークの検討

高野 泰洋[1]　白石 善明[1]　森井 昌克[1]

概要：本稿は，物理層・セキュリティを利用した Internet of Things (IoT) 無線ネットワークを検討する．Multi-input single-output (MISO) システムを想定したケース・スタディを通じて，情報理論的安全な無線伝送の必要条件が確認される．更に，チャネル・レシプロシティにおけるなりすましを抑止する通信プロトコルが検討される．

キーワード：Internet of Things (IoT)，物理層セキュリティ，秘匿チャネル容量，チャネル・レシプロシティ，情報理論的安全性．

A Study of IoT Networks using Wireless Physical Layer Security

Yasuhiro TAKANO[1]　Yoshiaki SHIRAISHI[1]　Masakatsu MORII[1]

Abstract: This paper studies Internet of Things' (IoT) wireless networks utilizing physical layer security. Case studies assuming a multi-input single-output (MISO) system confirm necessity conditions to perform information-theoretic secured wireless transmission. Moreover, a protocol to prevent an identity theft attack in channel reciprocity is discussed.

Keywords: Internet of Things (IoT), physical layer security, secrecy capacity, channel reciprocity, information-theoretic security.

1. はじめに

無線伝送は通信ノードの物理的な配置を自由にする．従って，多くの Internet of Things (IoT) 端末は無線伝送を用いた情報通信を行っている．しかし，無線伝送は常に第三者から傍聴されうる．従って，Bluetooth [1] 等の比較的近距離の無線通信を想定した伝送プロトコルであっても，セキュリティ向上のため暗号化に対応している．しかし，バッテリーレスかつメンテナンスフリーを目的としたセンサディバイスにとって，必ずしも高度な暗号化処理が実現できるとは限らない．

近年，第 5 世代移動通信を想定した大規模 Multiple-input multiple-output (MIMO) システム [2] が広く研究されている．多数のアンテナを利用する大規模 MIMO 伝送は，空間自由度を利用して，スペクトラム利用効率を向上させる．更に，多数の送信アンテナを用いたビームフォーミング伝送は，電波に指向性を持たせ，特定の通信相手のスループットを高めることを可能にする．そこで，大規模 MIMO 信号処理を想定し，情報理論的安全な通信を目指した物理層セキュリティが注目を集めている．物理層セキュリティは，従来の計算量的安全な暗号化の完全な代替手段を与えるものではない．しかし，両者を組み合わせることで，暗号化処理の軽量化，もしくは，更なるセキュリティ向上が可能になると期待される．

物理層セキュリティの概念や理論を紹介する文献は多数ある ([3], [4] 等)．しかし，現実的なシステム実装に起因する課題はまだ十分に議論されていない．そこで本稿は，ケース・スタディを通じて，情報理論的安全な無線伝送の動作原理を確認し，更に，その通信プロトコルについて検討する．

本稿の構成は次の通りである．第 2 章は物理層セキュリティを概説する．第 3 章は，Multiple-input single-output

[1] 神戸大学
Kobe University

(MISO) システムを想定し，情報理論的安全な伝送方法の原理を説明し，また，数値例を通じて，その実現可能性を議論する．第 4 章は，情報理論的安全な伝送を可能にするプロトコルを検討する．第 5 章は，本稿の結論をまとめる．

2. 物理層セキュリティ

2.1 秘匿チャネル容量 (Secrecy capacity)

Alice から Bob への情報伝送を Eve が傍聴しているとする．Alice と Bob の間の秘匿チャネル容量 $\mathcal{C}_S$ は，

$$\mathcal{C}_S = \mathcal{C}_B - \mathcal{C}_E \tag{1}$$

により定義される．但し，$\mathcal{C}_B$ と $\mathcal{C}_E$ は，それぞれ，Alice と Bob 間および Alice と Eve 間の非負のチャネル容量とする．秘匿チャネル容量 $\mathcal{C}_S$ は，情報理論的安全な通信が可能な伝送レートを示す．

2.2 物理層セキュリティにおける「情報理論的安全性」

本節は，秘匿チャネル容量 $\mathcal{C}_S$ と情報理論的安全性の関係を考察する．$\mathbf{m}(\mathcal{C})$ を 伝送レート $\mathcal{C}$ [bps/Hz] で送信される平文，その推定値 $\hat{\mathbf{m}}$ とする．**情報理論的安全性**は，秘匿チャネル容量 $\mathcal{C}_S$ を使って定義できる： $0 \le \forall\epsilon < 1$ と伝送レート $\mathcal{C}_E$ [bps/Hz] の受信信号 $\mathbf{r}(\mathcal{C}_E)$ に対し，

$$|\mathrm{P_r}\{\hat{\mathbf{m}} = \mathbf{m}(\mathcal{C}_B)\} - \mathrm{P_r}\{\hat{\mathbf{m}} = \mathbf{m}(\mathcal{C}_B) \mid \mathbf{r}(\mathcal{C}_E)\}| < \epsilon$$

を満たすよう，$\mathcal{C}_S = \mathcal{C}_B - \mathcal{C}_E > 0$ を決定できる．

この定義から分かるように，物理層セキュリティにおける情報理論的安全性は，暗号化による「安全」 – (鍵が無い限り) 暗号文を入手しても平文を解読できない – とは異なることに注意されたい．$\mathcal{C}_S > 0$ は， $\mathcal{C}_S \le 0$ でない (伝送情報が Eve へ筒抜けではない) ことを意味するのであって，Eve へ $\mathcal{C}_E$ の情報量が漏洩する．ところが，ターボ符号や Low-density parity-check (LDPC) 符号などのシャノン限界に漸近する伝送レート特性を持つ伝送路符号化を施して $\mathcal{C}_B$ のチャネル容量を使い切れば，Eve は漏洩した $\mathcal{C}_E$ の情報量から何も有意な情報を復号できない．

3. ケース・スタディ

3.1 信号モデル

図 1 に示す通り，Alice は長さ L_x のデータ・シンボルベクトル $\mathbf{x}(l)$ を $N \times 1$ MISO システムを使って Bob へ伝送する．スロット・タイミング l における Bob の受信シンボルベクトル $\mathbf{y}_B(l)$ は， フラットフェージング・チャネル $\mathbf{h}_B(l) = [h_{B,1}(l), \cdots, h_{B,N}(l)]^{\mathrm{T}}$ と Additive white Gaussian noise (AWGN) ベクトル[*1] $\mathbf{z}_B \sim \mathcal{CN}(\mathbf{0}_{L_x}, \sigma_{z,B}^2\mathbf{I}_{L_x})$ の

[*1] 簡潔な記述のためインデックス l を省略するが，熱雑音ノイズ $\mathbf{z}_B$ はスロット・タイミング毎に異なる． また，$\mathcal{CN}(\mu, \mathbf{\Sigma})$ は平均ベクトル μ, 分散行列 $\mathbf{\Sigma}$ の複素多変量正規分布を記す．

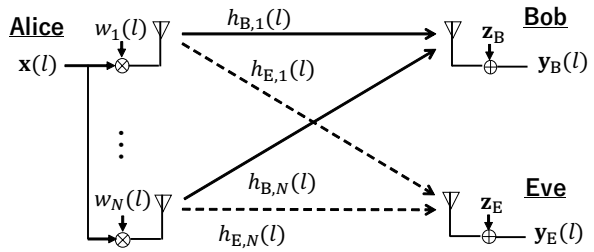

図 1 システムモデル．

影響を受け，

$$\mathbf{y}_B(l) = \mathbf{x}(l)\mathbf{w}^{\mathrm{T}}(l)\mathbf{h}_B(l) + \mathbf{z}_B \tag{2}$$

と書ける．ここで，$\mathbf{w}(l) = [w_1(l), \cdots, w_N(l)]^{\mathrm{T}}$ は送信重みベクトルである．同様に，傍聴者 Eve の受信信号 $\mathbf{y}_E(l) \in \mathbb{C}^{L_x}$ は，長さ N シンボルのチャネルベクトル $\mathbf{h}_E(l)$ と AWGN ベクトル $\mathbf{z}_E(l) \sim \mathcal{CN}(\mathbf{0}, \sigma_{z,E}^2\mathbf{I}_{L_x})$ に対し

$$\mathbf{y}_E(l) = \mathbf{x}(l)\mathbf{w}^{\mathrm{T}}(l)\mathbf{h}_E(l) + \mathbf{z}_E \tag{3}$$

である．

3.2 秘匿チャネル容量

Alice と Bob の間のチャネル容量 $\mathcal{C}_B$ と Alice と Eve の間のチャネル容量 $\mathcal{C}_E$ は，それぞれ，信号モデル (2)，(3) に対応して，

$$\mathcal{C}_B = \mathbb{E}\left[\log_2\left(1 + |\mathbf{w}^{\mathrm{T}}(l)\mathbf{h}_B(l)|^2\sigma_x^2/\sigma_{z,B}^2\right)\right] \tag{4}$$

$$\mathcal{C}_E = \mathbb{E}\left[\log_2\left(1 + |\mathbf{w}^{\mathrm{T}}(l)\mathbf{h}_E(l)|^2\sigma_x^2/\sigma_{z,E}^2\right)\right] \tag{5}$$

である．ここで，σ_x^2 は送信ベクトル $\mathbf{x}(l)$ の各要素の分散である．

Alice は，$\mathcal{C}_B$ を最大化するよう，定数 P の電力制約 $||\mathbf{w}(l)||^2 \le P$ の下で送信重み $\mathbf{w}(l)$ を最適化できる．送信重みの最適値 $\hat{\mathbf{w}}(l)$ は，

$$\begin{aligned}\hat{\mathbf{w}}(l) &= \arg\max_{\mathbf{w}} |\mathbf{w}^{\mathrm{T}}\mathbf{h}_B(l)|^2 \\ &= \mathbf{h}_B^*(l)/\sqrt{||\mathbf{h}_B(l)||^2}\end{aligned} \tag{6}$$

である．このとき， 秘匿チャネル容量は

$$\mathcal{C}_S = \mathbb{E}\left[\log_2 \frac{\sigma_{z,B}^2\sigma_{\mathbf{h},B}^2 + \sigma_x^2\sigma_{\mathbf{h},B}^4}{\sigma_{z,B}^2\sigma_{\mathbf{h},B}^2 + \sigma_x^2|\mathbf{h}_B^{\mathrm{H}}(l)\mathbf{h}_E(l)|^2/\alpha}\right] \tag{7}$$

と書ける． 但し，$\sigma_{\mathbf{h},B}^2 = \mathbb{E}[||\mathbf{h}_B(l)||^2]$，$\alpha = \sigma_{z,E}^2/\sigma_{z,B}^2$ である．

3.3 チャネル・レシプロシティ

送信重み (6) は $\mathbf{h}_B(l)$ を使って算出される．しかし，端末の移動を前提とする無線通信では， チャネルベクトル $\mathbf{h}_B(l)$ は変動しうる．従って，チャネル推定ベクトル $\hat{\mathbf{h}}_B(l)$ は通信中に推定しなければならない．そこで，Alice は Bob から送信された長さ L_p の既知のパイロット信号ベクトル

$\mathbf{p}_B$ を用いて $\hat{\mathbf{h}}_B(l)$ を推定する．[*2]

しかし，一般的な無線システムでは全二重伝送を想定しないため，$\mathbf{p}_B$ と $\mathbf{x}(l)$ は異なるスロット・タイミングに伝送される必要がある．電波伝搬の性質上，スロット間隔をチャネルのコヒーレンス時間より十分短く設定すれば，チャネルパラメータが緩やかに変動するとみなしてよい．チャネル・レシプロシティは，

$$\mathbf{h}_B(l) \approx \mathbf{h}_B(l-1) \tag{8}$$

なる近似に基づき算出した送信重みを用いたビームフォーミングを行う伝送手法である．チャネル・レシプロシティ伝送時の秘匿チャネル容量の上限は

$$\mathcal{C}_S \leq \mathbb{E}\left[\log_2 \frac{\sigma_{z,B}^2\sigma_{\mathbf{h},B}^2 + \sigma_x^2|\mathbf{h}_B^{\mathrm{H}}(l-1)\mathbf{h}_B(l)|^2}{\sigma_{z,B}^2\sigma_{\mathbf{h},B}^2 + \sigma_x^2|\mathbf{h}_B^{\mathrm{H}}(l-1)\mathbf{h}_E(l)|^2/\alpha}\right] \tag{9}$$

である．

3.4 数値例

秘匿チャネル容量 (9) はチャネルパラメータの性質や signal-to-noise ratio (SNR) に依存する．本節では，具体的なシステムパラメータを想定し，情報理論的安全な無線伝送の実現可能性を確かめる．

3.4.1 パラメータ設定

アンテナ数は，(Alice, Bob, Eve) の三者において $(8, 1, 1)$ である．キャリア周波数と伝送帯域幅は，それぞれ，2 GHz と 1 MHz とする．伝送路符号化のフレーム単位は $L_F = 10$ スロットで構成され，1 スロットの長さは $L_x = 1000$ シンボルとする．送信電力制限は $P \leq 1$ である．また，チャネルパラメータはレイリーフェージングに従うと想定する．更に，本稿では，理想的な演算精度でチャネル推定値が得られると仮定する．

3.4.2 秘匿チャネル容量の検証

図 2 は，Bob と Eve が 5 km/h で移動する場合の秘匿チャネル容量を示す．Bob と Eve の位置はフレーム毎にランダムに選ばれ，二者と Alice の距離は SNR に応じて決定されるとする．Bob と Eve が Alice から同一半径の位置に配置される場合，$\alpha = 1$，つまり，(Bob の SNR)/(Eve の SNR) = 0 dB となる．このとき，図 2 の曲線: $\alpha = 0$ dB が示す通り，秘匿チャネル容量 (7) は全 SNR 領域にて $\mathcal{C}_S > 0$ が成り立つ．また，秘匿チャネル容量 $\mathcal{C}_S$ は，Bob の SNR が増加しても 3.8 [bps/Hz] に飽和することが分かる．これは，SNR 増加に伴い $\sigma_{z,B}^2 \to 0$ となるが，

$$\mathcal{C}_S \leq \mathbb{E}\left[\log_2 \frac{\sigma_{\mathbf{h},B}^4}{|\mathbf{h}_B^{\mathrm{H}}(l)\mathbf{h}_E(l)|^2/\alpha}\right] = 3.8 \tag{10}$$

[*2] 例えば，Aice の $N \times L_p$ の受信シンボル行列 $\mathbf{Y}_A(l) = \mathbf{h}_B(l)\mathbf{p}_B^{\mathrm{T}} + \mathbf{Z}_A$ に対し，Least squares (LS) チャネル推定値は $\hat{\mathbf{h}}_B(l) = \mathbf{Y}_A(l)\mathbf{p}_B^* \cdot (\mathbf{p}_B^{\mathrm{T}}\mathbf{p}_B^*)^{-1}$ により与えられる．

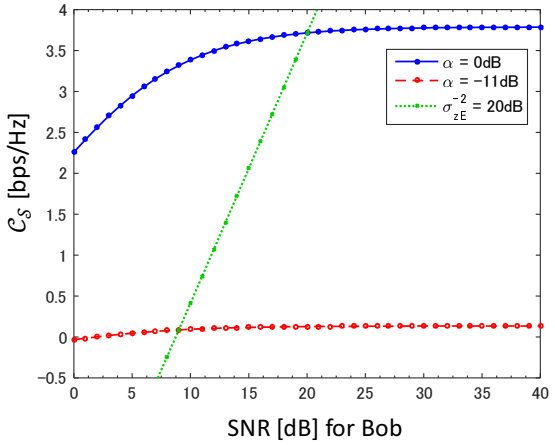

図 2　Rayleigh フェージングにおける秘匿チャネル容量 (7).

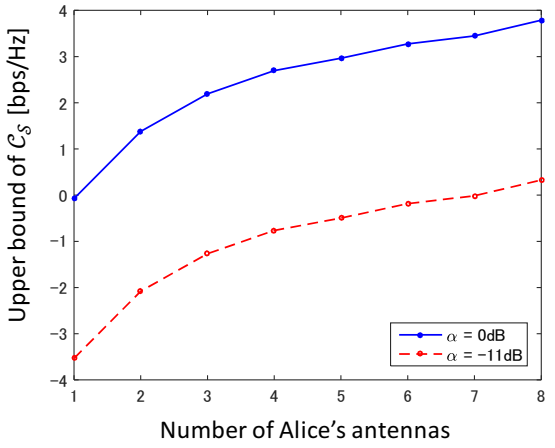

図 3　秘匿チャネル容量の上限 (10).

が成り立つためである．図 3 に示す通り，秘匿チャネル容量の上限は，Alice のアンテナ数に比例する．つまり，秘匿チャネル容量の上限は，チャネルパラメータの相関特性に加えて，Alice のアンテナ数と Bob と Eve の SNR 比を表すパラメータ α により決定される．

図 2 において，直線: $\sigma_{z,E}^{-2} = 20$ dB は，Eve の SNR を 20 dB に固定した際の秘匿チャネル容量を示す．図 2 から分かるように，この直線は SNR $= 8 < 20 - 11$ dB にて $\mathcal{C}_S < 0$ となる．即ち，Eve が Alice に近づき $\alpha < -11$ dB となる場合，情報理論的安全な無線伝送は実行できない．この問題の解決策は，図 3 から分かるように，Alice のアンテナ数を増やすことである．

次に，チャネル・レシプロシティが前提とする近似 (8) について検証する．図 4 に示す通り，移動速度が 5 km/h のとき，秘匿チャネル容量 (7) と (9) は一致する．これは，移動速度が低速であるとき，近似 (8) が正確なためである．しかし，移動速度が高速になると，(8) の近似誤差は無視できない．図 4 において，移動速度が 50 km/h のとき，秘匿チャネル容量 (9) は (7) より 0.3 [bps/Hz] 劣化する．従っ

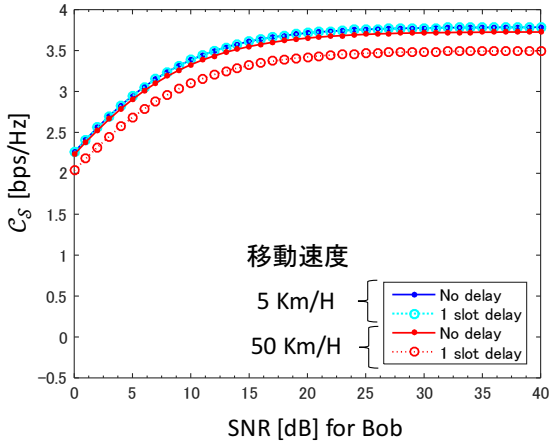

図 4　秘匿チャネル容量 (7) : No delay と (9) : 1 slot delay の比較.

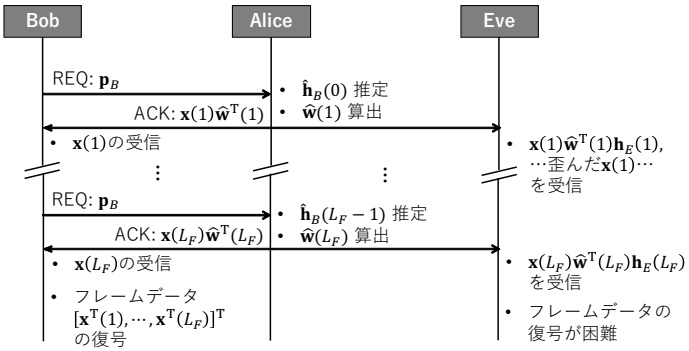

図 5　チャネル・レシプロシティのプロトコル・シーケンス.

て，高速移動を想定する場合，スロット間隔 L_x を短くして，(8) の近似精度を改善する必要がある．

4. プロトコルの検討

4.1 チャネル・レシプロシティを実現するプロトコル

図 5 により，チャネル・レシプロシティを実行するために必要な最低限のプロトコル・シーケンスを説明する．通信中に変化するチャネルベクトルの推定値 $\hat{\mathbf{h}}_B(l)$ 更新のため，毎スロット，Bob は Alice に対しパイロット $\mathbf{p}_B$ を伝送する．近似 (8) とチャネル推定が十分高精度であれば，Alice から重み付け送信された信号 $\mathbf{x}(l)\hat{\mathbf{w}}^{\mathrm{T}}(l)$ は，Bob には

$$\mathbf{y}_B(l) = \sqrt{||\mathbf{h}_B(l)||^2}\cdot\mathbf{x}(l) + \mathbf{z}_B$$

として受信される．つまり，Bob はチャネル推定およびチャネル等化を行う必要がない．

なお，送信信号 $\mathbf{x}(l)\hat{\mathbf{w}}^{\mathrm{T}}(l)$ は Eve へ漏洩するが，その情報量は $\mathcal{C}_E < \mathcal{C}_B$ となる．従って，Eve はフレームデータを正しく復号することが困難である．また，Eve はパイロット $\mathbf{p}_B$ 信号を受信し，Eve と Bob 間のチャネルパラメータ $\mathbf{h}_{BE}(l)$ を推定できる．しかし，(9) に示した通り，秘匿チャネル容量は $\mathcal{C}_S$ は $\mathbf{h}_B(l)$ と $\mathbf{h}_E(l)$ により決定され，$\mathbf{h}_{BE}(l)$ には依存しないことに注意されたい．

4.2 課題

しかしながら，図 5 に示したプロトコルは，妨害波やなりすましに対し脆弱である．

4.2.1 妨害波

Eve は Bob の Request (REQ) 伝送時に妨害波を送信し Alice のチャネル推定 $\hat{\mathbf{h}}_B(l)$ を妨げることができる．この攻撃に対し，Alice と Bob は，先ず, 妨害波の存在を検出しなければならない．能動的な攻撃者の検出は [5] 等で議論されている．次に，Alice は干渉キャンセル処理 ([6] 等) により，問題を改善することができる．しかし，干渉キャンセル処理の多くはマルチアンテナを前提とする．従って，Bob が 1 本アンテナで受信している場合，Alice の Acknowledgement (ACK) 伝送時の妨害波への対策は，再送処理が挙げられる．

4.2.2 なりすまし

図 5 のシーケンスにおいて，Bob の REQ 前に，Eve がパイロット $\mathbf{p}_B$ を送信することで，容易に Eve は Bob になりすませる．あるいは，Eve は Bob の REQ を受けて，Alice になりすまして偽の ACK を Bob に通知することで，正常な通信を阻害できる．

この問題への対策として，認証フェーズを追加したプロトコル・シーケンスを図 6 に示す．認証フェーズにおいて，Alice と Bob はそれぞれの公開鍵 (k_p^A, k_p^B) を事前に共有していると仮定する．また，平文 m，公開鍵 k_p，秘密鍵 k_s に対し，$e = \mathrm{E}(m, k_p)$ を任意の非対称暗号化関数，対応する復号関数を $m = \mathrm{D}(e, k_s)$ と記す．認証フェーズの詳細は，次の通りである：

i) Bob は Alice の公開鍵 k_p^A を使い，自身の識別番号 ID_B を $e_{\mathrm{REQ}} = \mathrm{E}(\mathrm{ID}_B, k_p^A)$ により暗号化する．
ii) Bob は デフォルトのパイロット信号 $\mathbf{p}_{\mathrm{REQ}}$ と e_{REQ} を Alice へ送る．
iii) Alice は，自身の秘密鍵 k_s^A を使い，e_{REQ} から識別番号 ID_B を復号して Bob の要求を検知する．
iv) Alice は，Bob の要求を受けて，乱数 r を生成する．
v) Alice は，Bob の公開鍵 k_p^B を使い $e_{\mathrm{ACK}} = \mathrm{E}(r, k_p^B)$ により乱数を暗号化する．
vi) Alice は，$\mathbf{p}_{\mathrm{REQ}}$ に対応する受信信号から送信重み $\hat{\mathbf{w}}(0)$ を算出する．
vii) Alice は，送信重み $\hat{\mathbf{w}}(0)$ を使って e_{ACK} を Bob へ送る．
viii) Bob は，自身の秘密鍵 k_s^B を使い，乱数 $r = \mathrm{D}(e_{\mathrm{ACK}}, k_s^B)$ を復号する．
ix) これにより，Alice と Bob は 乱数 r を共有する．
x) ハッシュ値 $\mathcal{H}(r, l) = s_{\mathcal{H}}$ をシードにして決定される擬似乱数 $\mathrm{PN}(s_{\mathcal{H}})$ に基づき，Alice と Bob は パイロット信号 $\mathbf{p}_B(l)$ を決定する．
xi) 以後, 共有された $\mathbf{p}_B(l)$ を使い, Alice と Bob はチャネル・レシプロシティ伝送を行う．

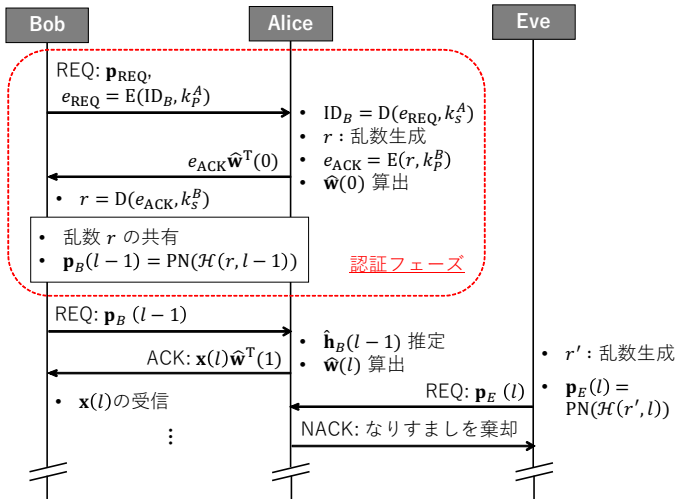

図 6　認証フェーズを追加したプロトコル・シーケンス．

図 6 に示す通り，認証フェーズにより，Alice は 共有されたパイロット信号により，Eve のなりすましを棄却できる．従って，Eve が Bob になりすまして Alice から情報を盗み出すことに成功する確率は $|\{\mathrm{PN}(s_{\mathcal{H}}) \mid \forall s_{\mathcal{H}}\}|^{-L_F}$ である．つまり，なりすましを防止するためには，広い値域を持つ擬似乱数と十分大きな L_F を採用する必要がある．

従来のセキュアな無線伝送は， 伝送路符号化の上で，プレゼンテーション層などの上位レイヤにおいて認証データやペイロード・データの暗号化を実施していた．一方，図 6 のプロトコルは，Alice から Bob へのデータベクトル $\mathbf{x}(l)$ に対し，伝送路符号化のみ行う．暗号化は，認証フェーズのみ実施され，実データ $\mathbf{x}(l)$ に対しては利用されていないことに注意されたい．

5. まとめ

本稿は，無線物理層セキュリティを利用するための必要条件を確認し，そのプロトコルについて検討した．IoT ネットワークを想定した MISO システムでのケース・スタディを通じて，情報理論的安全な無線伝送が成立するための必要条件を確認した．具体的には，

- 送信者 Alice のアンテナ数が多いこと，
- 正規受信者 Bob と傍聴者 Eve の SNR 比が所定値より大きいこと，
- スロット間隔 L_x がチャネルのコヒーレント時間より小さいこと，

が必要である．これらの条件下で，秘匿チャネル容量の上限が (10) により決定されるチャネル・レシプロシティ伝送が実行可能となる．しかし，チャネル・レシプロシティ伝送は，なりすましの脆弱性がある．その対策として，本稿は，相互認証を考慮したプロトコルを検討した．また，プロトコルの安全性を高めるために，

- 1 フレームのスロット分割数 L_F が大きいこと，
- パイロット信号生成に利用する擬似乱数が広い値域を持つこと，

の必要性を議論した．

本稿では，無線物理層セキュリティの動作原理を確認するため，MISO システムに注目した．今後の課題として，本研究は，Eve が多数のアンテナで傍聴しうることを考慮し，MIMO システムを想定した物理層セキュリティの安全性評価に取り組む．

謝辞　本研究は JSPS 科研費 17K06423 および電気通信普及財団の助成を受けたものである．

参考文献

[1] C. Bisdikian. An overview of the Bluetooth wireless technology. *IEEE Communications Magazine*, Vol. 39, No. 12, pp. 86–94, Dec 2001.
[2] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta. Massive MIMO for next generation wireless systems. *IEEE Communications Magazine*, Vol. 52, No. 2, pp. 186–195, February 2014.
[3] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen. Physical layer security in wireless networks: a tutorial. *IEEE Wireless Communications*, Vol. 18, No. 2, pp. 66–74, April 2011.
[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys Tutorials*, Vol. 16, No. 3, pp. 1550–1573, Third 2014.
[5] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, and F. Rusek. Detection of active eavesdroppers in massive MIMO. In *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, pp. 585–589, Sept 2014.
[6] N. Zhao, F. R. Yu, M. Jin, Q. Yan, and V. C. M. Leung. Interference alignment and its applications: A survey, research issues, and challenges. *IEEE Communications Surveys Tutorials*, Vol. 18, No. 3, pp. 1779–1803, thirdquarter 2016.