ランプ型秘密分散法を用いた秘密分散伝送における送信情報の秘匿性向上に関する考察

松本樹里[1,a)]　山中仁昭[1,b)]

概要：本稿では，著者らがこれまでに検討を進めてきた無線空間内における秘密分散伝送法において，情報の分散手法としてランプ型秘密分散法を適用することを検討する．ランプ型秘密分散法とは，情報の秘匿性の劣化を許容することで伝送効率の向上を図る情報の分散手法である．われわれは，ランプ型秘密分散法を適用した際に生じる秘匿性の劣化を，無線空間内での分散情報の伝送方法を工夫することで補うことを検討している．本稿では，まず，ランプ型秘密分散法を適用した際の秘匿性の劣化量を情報理論的な観点から明らかにする．その上で，そうした劣化量を低減する手法について考察する．

1. はじめに

ユーザ周辺の情報伝達を支える通信ネットワークとして無線 LAN に代表されるプライベートな無線ネットワークが広く普及している．われわれは，こうした無線ネットワークにおける盗聴対策として，送信情報を無線空間内において分散して伝送することにより，送信情報の秘匿性を向上する方式を提案してきた [1][2]．提案法では，まず，秘密分散法に基づいて元情報をそれ単独では意味をなさない情報へ分割する．続いて，無線伝搬路のマルチパス性に着目し，送信ノードから受信ノードへ至る幾つかのパスを選択した後，選択したパスへ情報を分散して伝送する．秘密分散法は情報の分散管理手法の一つで，(k，n) 閾値法とも呼ばれる [3]．元情報を n 個の情報に分散して管理し，これら n 個の分散情報のうち k 個以上あれば元情報を誤りなく復元できるが，k 個未満であれば元情報に関する情報を一切得ることができない特徴を有する．このような秘密分散法を適用し，送信情報を無線空間内で分散して伝送することにより，盗聴者は k 個以上の分散情報を集めなければ元情報を復元することができない．そのため，送信者は k をパラメータとして無線環境に合わせて設定することにより，伝送中における送信情報の秘匿性を向上できる．

秘密分散法は無線ネットワーク内において情報を秘密裏に伝送するための情報の分割手法として有効な手段である [4][5]．しかしながら，上記のような (k，n) 閾値型の特徴を満たすためには，個々の分散情報の情報量（エントロピー）は元の送信情報のそれ以上でなければならないことが知られている [6]．つまり，送信情報を分割することにより，その分割数に比例して送信情報全体の情報量は増大する．その結果，送信情報を伝送するために必要な情報ビット数が増大し，伝送効率が劣化する問題が生じる．

こうした問題に対してランプ型秘密分散法が提案されている [7]．ランプ型秘密分散法とは，k 個未満の分散情報に対しても，送信情報の一部が漏洩することを許す手法であり，秘匿性の劣化と引き換えに伝送効率の向上を図る手法である．本稿では，ランプ型秘密分散法に基づいて分散伝送を行う際の基礎検討として，まず，ランプ型秘密分散法を用いることによる秘匿性の劣化量をシミュレーション実験により明らかにする．その上で，そうした劣化量を低減する手法について考察する．

2. 秘密分散伝送の概要

一般に，無線伝搬路は複数のパスが混在するマルチパス伝搬路となる．われわれは，これらのマルチパスを利用し，送信／受信ノードのアンテナ指向性を制御することにより，無線空間内において情報を分散して伝送する手法を提案してきた．図 1 はその分散伝送の様子を示している．本手法では，まず，送信ノードから受信ノードへ至る幾つかのパスを選択する．続いて，送信／受信ビームを制御することにより，選択したパスの周囲に複数の伝送路を形成し，複数の伝送路へ情報を分散して伝送する．このとき，送信情報をそれ単独では意味をなさない情報へ分割して伝送することにより，たとえその一部が漏洩したとしても元情報の秘匿性を保つことができる．

[1] 広島国際大学工学部情報通信学科
Hirokoshingai 5-1-1, Kure, Hiroshima 737–0003, Japan
[a)] si11044@ym.hirokoku-u.ac.jp
[b)] m-yamana@it.hirokoku-u.ac.jp

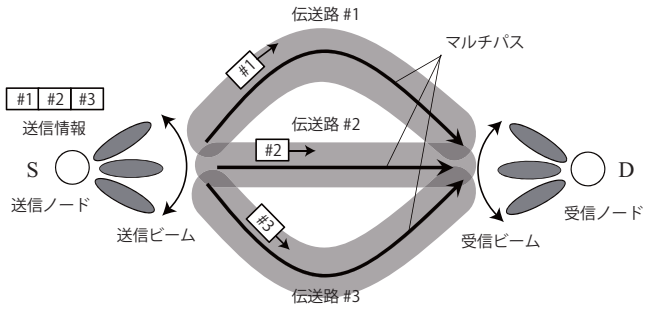

図 1 分散伝送の様子

2.1 （k，n）閾値型秘密分散法の課題点

（k，n）閾値型秘密分散法を適用して送信情報を分割しておくことにより，盗聴者は k 個以上の分散情報を集めない限り元の送信情報を得ることができない．そのため，経路が異なる複数のパスを利用し，送信情報を無線空間内に広く分散して伝送させることにより伝送中の情報漏洩の危険性を軽減できる．

しかしながら，（k，n）閾値型秘密分散法では以下の関係を満たす必要があることが知られている．ただし，X は元情報，$X_1, X_2, ..., X_n$ は分散情報であり，$H(\cdot)$ はエントロピー関数である．

$$H(X) \leq H(X_k) \quad (k = 1, 2, ..., n) \qquad (1)$$

式（1）は各分散情報の情報量（エントロピー）は元情報のそれ以上でなければならないことを示しており，分散情報の伝送には元情報よりも多くの情報ビットが必要となることを示している．つまり，情報の分散数に比例して送信情報を伝達するために必要となる総ビット数が増大するため，伝送効率が劣化する．

3. ランプ型秘密分散法の適用

3.1 ランプ型秘密分散法

ランプ型秘密分散法とは，（k，n）閾値型秘密分散法の伝送効率の向上を目的として提案された手法である [7]．（k，L，n）閾値型秘密分散法とも呼ばれ，n 個の分散情報のうち k 個以上あれば元情報を誤りなく復元できるが，$k - L$ 個未満であれば元情報に関する情報を一切得ることができず，$k - t$ （$1 \leq t \leq L - 1$）の分散情報からは t が小さくなるにつれて段階的に元情報に関する一部の情報が得られる（漏洩する）という特徴を有する．こうしたランプ型秘密分散法を用いることにより，個々の分散情報の情報量は $1/L$ に低減されるため，伝送効率を L 倍に向上できる．すなわち，ランプ型秘密分散法は，k 個未満の分散情報からでも元情報に関する一部の情報漏れを許すことにより，そうした秘匿性特性の劣化と引き換えに伝送効率を向上する手法である．

3.2 ランプ型秘密分散法による秘匿性の劣化量の評価

ランプ型秘密分散法を用いることにより，伝送効率を向上できる．その一方で，送信情報の秘匿性が犠牲となる．本節では，伝送効率の向上と引き換えに生じる送信情報の秘匿性の劣化量を情報理論的な観点から明らかにする．

（k, n）閾値型秘密分散法において，k が n と等しい場合を満場一致型と呼ぶ．満場一致型はすべての分散情報がなければ元情報が復元できないため，（k, n）閾値型秘密分散法において最も送信情報の秘匿性の高い情報の分割手法である．本稿では，（k, n）閾値型秘密分散法として満場一致型を前提として議論を進める．このとき，満場一致型秘密分散法（（n，n）閾値型秘密分散法）では伝送効率は $1/n$ に劣化する．こうした伝送効率の劣化をランプ型秘密分散法にて解消するためには，L を n と等しく設定すればよい．本稿では，ランプ型秘密分散法として（n，n，n）閾値型秘密分散法を採用し，両者の秘匿性の違いを検証する．

3.2.1 情報漏洩量の数式表現

一般に情報の漏洩量は相互情報量によって評価できる [8]．今，送信情報を X，分散情報を $X_1, X_2, ..., X_n$ とする．また，個々の分散情報に対応する受信情報を $Y_1, Y_2, ..., Y_n$ とし，これらの情報から復元される情報ををを Y とする．このとき，個々の分散情報の漏洩量は X_k と Y_k の相互情報量（$I(X_k; Y_k)$ ）として評価できる．さらに，こうした相互情報量を基に，送信情報の漏洩量は以下のように求められる．なお，満場一致型，ランプ型の違いによって，分散情報や受信情報が異なる．そのため，満場一致型については分散情報を $Xt_1, Xt_2, ..., Xt_n$，それに対する受信情報を $Yt_1, Yt_2, ..., Yt_n$ とし，ランプ型についてもそれぞれ同様に $Xr_1, Xr_2, ..., Xr_n$，$Yr_1, Yr_2, ..., Yr_n$ とした．

満場一致型秘密分散法（（n, n）閾値型）

（n，n）閾値法ではすべての分散情報がなければ元情報に関する情報が一切得られない．そのため，元情報の漏洩量は最も小さい分散情報の漏洩量として求められる．

$$I(X; Y) = \min_k I(Xt_k; Yt_k) \qquad (2)$$

ランプ型秘密分散法（（n, n, n）閾値型）

（n, n, n）閾値型では，一つの分散情報から元の送信情報に関する一部の情報が漏洩し，その漏洩量は分散情報の個数に比例して大きくなる．そのため，元情報の漏洩量は個々の分散情報の漏洩量の和として求められる．

$$I(X; Y) = \sum_k I(Xr_k; Yr_k) \qquad (3)$$

なお，ランプ型秘密分散法の特徴より，ランプ型秘密分散法では個々の分散情報の情報量は満場一致型秘密分散法のそれの $1/L$（本検討では $L = n$）となるため，次式が成立する．

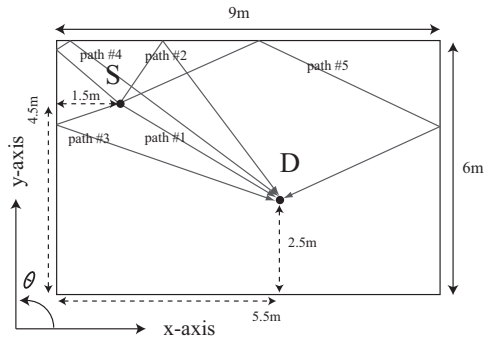

図 2 伝搬路モデル

表 1 パスの利得と放射角

Path number	♯1	♯2	♯3	♯4	♯5
Gain（dB）	0	-3.6	-4.4	-6.0	-9.6
AOD（deg.）	327.3	56.3	199.1	141.1	24.6

$$H(Xr_k) = \frac{1}{n} H(Xt_k) \tag{4}$$

そのため，同じ伝送品質の無線環境においては，ランプ型秘密分散法における分散情報の漏洩量は，満場一致型秘密分散法のそれの $1/n$ となる．

$$I(Xr_k; Yr_k) = \frac{1}{n} I(Xt_k; Yt_k) \tag{5}$$

3.2.2 シミュレーション実験による評価

ランプ型秘密分散法による秘匿性の劣化量を計算機シミュレーションにより検証した．ただし，伝送する分散情報は 2 値情報と仮定した．この場合，分散情報 X_k の漏洩量（$I(X_k; Y_k)$）は伝送誤り P_k を用いて次式にて求められる [9]．

$$I(X_k; Y_k) = 1 + P_k \log_2 P_k + (1 - P_k) \log_2 (1 - P_k) \tag{6}$$

本検討では，上式により，まず，伝送誤りから各分散情報の漏洩量を求めた上で，続いて，(2)，(3) 式により満場一致型，ランプ型秘密分散法を用いた際の送信情報の漏洩量を算出し，ランプ型秘密分散法を用いることによる秘匿性の劣化量を評価した．

図 2 に本検討で用いた伝搬路モデルを示す．本検討では長方形の室内環境を想定し，室内の伝搬路特性を壁面での反射を考慮したレイトレース法に基づいてモデル化した．レイトレース法を用いることでパスが伝搬する経路を正確に求めることができる [10]．図 2 にレイトレース法によって算出したパスの経路，表 1 に各パスの特性として，伝搬利得，送信ノードにおける放射角（angle of departure：AOD）を示す．ただし，伝搬利得は第 1 パスを基準とした正規化利得である．本検討では，図 2 に示す 5 つのパスを使い，満場一致型秘密分散法としては，(5,5) 閾値型を，ランプ型秘密分散法としては（5, 5, 5）閾値型を適用し検討を行った．

図 3，図 4 に満場一致型秘密分散法，ランプ型秘密分散法

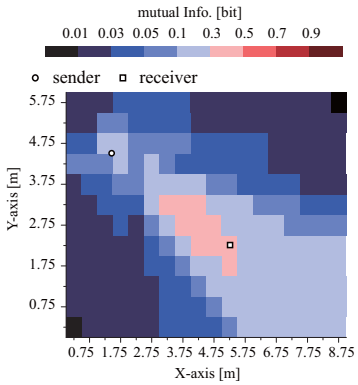

図 3 送信情報の漏洩量（w/ 満場一致型秘密分散法）

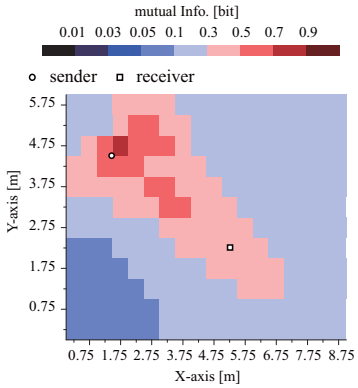

図 4 送信情報の漏洩量（w/ ランプ型秘密分散法）

をもちいた場合の伝搬路モデル内全域における送信情報の漏洩量を示す．両図は一情報辺りの漏洩量を表しており，送信情報を 2 値情報としたため，漏洩する情報量の最大値は 1 [bit] である．両図の結果より，ランプ型秘密分散法を用いることで，室内の広い領域で漏洩する情報量が増加し，送信情報の秘匿性が劣化していることが確認できる．こうした秘匿性の劣化はランプ型秘密分散法を用い，伝送効率を向上することによって生じる代償である．

4. 送信情報の秘匿性向上に関する検討

満場一致型秘密分散法を用いた場合，送信情報の漏洩量は各分散情報の漏洩量のうち，最も小さい漏洩量となる．そのため，情報の分散数を増やしても，新たな分散により情報の漏洩量が増すことはなく，送信情報の秘匿性が低下することはない．これに対して，ランプ型秘密分散法を用いた場合では，送信情報の漏洩量は各分散情報の漏洩量の和となる．漏洩量の大きい分散情報によって元の送信情報の漏洩量が増大するため，どのように情報を分散して伝送するか，情報を分散させるパスを慎重に検討する必要がある．

われわれは，ランプ型秘密分散法を用いて情報を分散して伝送する際の適切なパスの選択方法について検討を進めている．本稿では，その一検討として，パスの伝搬利得の違いに注目し，情報を分散するパスを伝搬利得の高いパス

に限ることの効果を検討する．

4.1 シミュレーション実験による評価

一般に，無線伝搬路内に存在するパスは，その伝搬距離や反射回数の違いによって様々であり，その周囲に形成される伝送路の広がりはパスの伝搬利得によって異なる．パスの伝搬利得が大きいほど送信電力を低減できるため，伝送路はパスに沿って狭く形成される．逆に，パスの伝搬利得が小さくなるほど，その広がりが大きくなる．広がりの大きい伝送路は，広い範囲に対して大きな量の情報を漏洩させるため，秘密伝送の観点からはそうしたパスへ情報を分散すべきではない．本節では，こうした考えに基づき，電力の高いパスに限って情報を分散することの送信情報の秘匿性向上の効果をシミュレーション実験によって評価する．

図 5 に分散伝送に用いるパスとして，図 2 に示す 5 本のパスのうち伝搬利得の高いパスから，(a) 5 パス，(b) 4 パス，(c) 3 パス，(d) 2 パスを選択したときの伝搬路モデル内における送信情報の漏洩量を示す．図 5 より，分散伝送に用いるパスを (a) 5 パスから (d) 2 パスへと減少させ，伝搬利得の高いパスのみへ情報を分散することで，送受信ノードから離れた領域において漏洩する情報量が減少し，送信情報の秘匿性が向上できることが分かる．特に，分散伝送に用いるパスを (a) 5 パスから (b) 4 パスとしたときの特性の改善量が大きい．これは，第 5 パスの伝搬利得が小さく，その周囲に形成される伝送路の広がりが大きいためであり，こうしたパスを通して広い範囲に大きな情報が漏洩するためであると考えられる．

一方で，分散伝送に用いるパスを少なく制限することによって，送受信ノードの周辺において漏洩する情報量が増大し，送信情報の秘匿性が劣化する領域が確認できる．特に，(d) においては (c) に対し送信ノードの周辺において送信情報の秘匿性が劣化する領域が目立つ．これは，情報の分散数を制限することにより，ある偏った方向に大きな情報が伝送される為である．

5. まとめ

本稿では，われわれがこれまでに検討してきた無線空間内における秘密分散伝送法において，ランプ型秘密分散法による送信情報の漏洩量を定式化し，情報理論的な観点から (k, n) 閾値型秘密分散法を用いた場合との秘匿性の違いを明らかにした．その上で，送信情報の秘匿性を向上するための一検討として，分散伝送に用いるパスを伝搬利得の高いパスに限ることにより，送信情報の秘匿性を向上できることを示した．無線空間内に形成される伝送路の広がりは均一ではなく，パスの伝搬利得によって様々なに異なる．今回得られた結果は，こうした伝送路の物理的な特徴を踏まえて情報を分散して伝送することが，送信情報の秘匿性を向上する上で有効であることを示している．

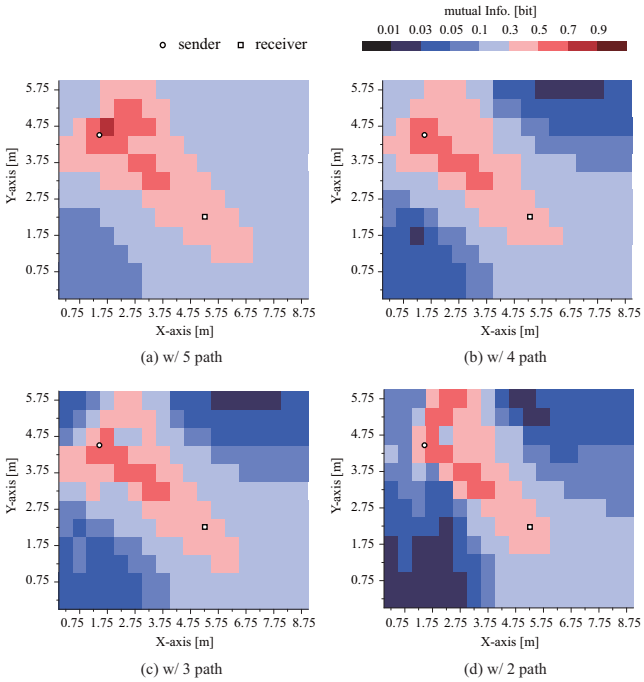

図 5 情報を分散するパスを変化させたときの送信情報の漏洩量

なお，本稿では，(k, n) 閾値型秘密分散法として (n, n) 閾値法を，ランプ型秘密分散法として (n, n, n) 閾値法に限って検討を行った．今後は両者を (k, n) 閾値法，(k, L, n) 閾値法として，より一般化した検討を行う予定である．

参考文献

[1] 山中仁昭，宮本伸一，三瓶政一：秘密分散法に基づくセキュアな無線通信リンクの形成－狭ビーム形成の効果とその弊害，情報処理学会論文誌，Vol.54, No.12, pp.2440–2450 (2013).

[2] 山中仁昭，宮本伸一，三瓶政一：セキュアな無線リンクを形成するための送受信ビームフォーミングによる分散伝送路形成法，Vol.55, No.2, pp.838–848 (2014).

[3] Shamir, A.: How to Share a Secret, *Communications of the ACM*, Vol.22, No.11, pp.612–613 (1979).

[4] Lou, W. and Fang, Y.: A Multipath Routing Approach for Secure Data Delivery, *Proc.MILCOM 2001*, pp.1467-1473 (2001).

[5] Berman, V. and Mukherjee, B.: Data Security in MANETs using Multipath Routing and Directional Transmission, *Proc. ICC 2006*, pp.2322-2328 (2006).

[6] Karnin, E.D., Greene, J. and Hellman, M.E.: On secret sharing systems, IEEE Trans. on Inform. Theory, Vol.29, No.1, pp.35-41 (1983).

[7] 山本博資：(k, L, n) しきい値秘密分散システム，電子情報通信学会論文誌，Vol.J68-A，No.9，pp.945-952 (1985).

[8] Cover, T.M. and Thomas, J.A.: *Elements of Information Theory*, Wiley (1938).

[9] 北野隆康，岩井誠人，笹岡秀一：複数アンテナからの干渉波送信制御を用いた秘密通信方式，電子情報通信学会論文誌，Vol.J92-B, No.9, pp.1362-1372 (2009).

[10] Seidel, S.Y. and Rappaport, T.S.: Site-specific propagation prediction for wireless in-building personal communication system design," *IEEE Trans. on Veh. Technol.*, Vol.43, No.4, pp.879-891 (1994).