様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月 ２６ 日現在

機関番号：８２７２７
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ０６３７５

研究課題名（和文）物理層のセキュリティと秘密分散を用いた通信システムの情報保護強化に関する研究

研究課題名（英文）A security enhancement technique for wireless communications based on physical layer secrecy coding and secret sharing

研究代表者

山嵜　彰一郎（YAMASAKI, shoichiro）

独立行政法人高齢・障害・求職者雇用支援機構職業能力開発総合大学校（能力開発院、基盤整備センター）・能力開発院・教授

研究者番号：６０６４８９６３

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：　(k, n)しきい値法の秘密分散は，情報をn個のシェアと呼ばれる情報に分散させ，k個以上のシェアを集めなければ元の情報を再構成できないようにシェアを構成することにより，情報の紛失と漏えいを抑制する方式である，一方，物理層のセキュリティは，基地局から端末への無線通信において，目標端末の受信条件を良好にし，かつ，目標端末以外の端末の受信条件を劣悪にするように伝送処理を実施することにより，情報の漏えいを抑制する方式である．本研究では，組織リードソロモン符号を用いた秘密分散と，ベクトルコーディングを用いた物理層のセキュリティを無線パケット通信の情報保護に適用した構成例を提案しその特性を明確にした．

研究成果の学術的意義や社会的意義
　秘密分散に基づく情報管理においてシェアの配信を伴う場合，シェアが非正規のユーザにより通信路上で取得される危険がある．このような状況を考慮して，本研究では，正規のユーザにおける分散されたシェアから情報を再構成するときの条件と比較して，非正規のユーザにおけるその条件が不利になるような秘密分散の工夫と，無線環境の情報配信を前提に，物理層の伝送処理により非正規ユーザにおける信号受信品質を劣化させる工夫を施した情報管理方式を提案し評価したことに学術的意義がある．
　第５世代無線通信，あるいは，それ以降の無線通信に応用し得る情報保護方式とシステムを提案していることに社会的意義がある．

研究成果の概要（英文）：　Secret sharing is a method to protect information for security. The information is divided into n shares, and the information is reconstructed from any k shares but no knowledge of it is revealed from k-1 shares. Physical layer security is a method to yield a favorable receive condition to an authorized destination terminal in wireless communications.
　In this study, we propose secure wireless packet communications with the secret sharing based on systematic Reed-Solomon coding and the physical layer security based on vector coding. The secret sharing based on Reed-Solomon coding yields a favorable receive condition to the authorized destination terminal. And the physical layer security based on vector coding implements a single-antenna system and a multi-antenna system. The validity of the proposed scheme was shown by computer simulations.

研究分野：通信工学

キーワード：情報セキュリティ　秘密分散　物理層のセキュリティ　リードソロモン符号　無線パケット通信

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

無線通信システムでは，基地局を中心とした通信エリアが設定され，基地局と端末の間で無線信号を用いた情報伝送が行われる．通信エリア内に，正規の受信者の端末以外に非正規の受信者の盗聴端末が存在すると，盗聴端末への情報漏えいを発生する危険性から，情報漏えいへの対処が必須となっている．

従来から，情報漏えいへの対策として，情報の暗号化が広く実用化されてきた．情報の暗号化通信では暗号に用いられる秘密鍵の保護が重要であり，秘密分散が秘密鍵の漏えいと消失を抑制する技術として注目されている．秘密分散のひとつの方式である(k, n)しきい値法は，秘密情報を n 個のシェアと呼ばれる分散情報に分散する．このとき，k 個 $(k < n)$ 以上のシェアからは秘密情報を完全に再構成でき，$k - 1$ 個以下のシェアからは秘密情報に関する何の情報も漏えいしないように，シェアは設定される．従って，盗聴者の端末は n 個のうち $k - 1$ 個までシェアを取得した場合でも秘密情報に関する情報を得られず，一方，正規の利用者の端末は n 個のうち $n - k$ 個までのシェアを消失することが起こった場合でも秘密情報を再構成可能である．

一方，近年，盗聴端末において無線信号の受信品質を著しく劣化させることにより，情報漏えいを抑制する技術の研究が進んでおり，送信機と受信機の間で複数アンテナを用いた伝送技術に基づく方式が実現法のひとつであり，このような情報保護方式は物理層のセキュリティ技術と呼ばれ，第５世代 (5G) 無線通信の研究開発においても注目されている．

情報通信において，秘密分散は上位層の技術，物理層のセキュリティは下位層の技術であり，それぞれ独立して研究開発がなされてきた．

２．研究の目的

上位層における符号化を基盤とした秘密分散の性能改善方式と，下位層における符号化を基盤とした物理層のセキュリティの性能改善方式を各々開発することと，これらの性能改善方式を連携することにより，無線通信システムの情報保護の強化方式を開発し特性を評価し有効性を確認することを研究目的とする．

３．研究の方法

(k, n)しきい値法の秘密分散は，組織リードソロモン符号，あるいは，非組織リードソロモン符号により実現することができるが，このうち，組織リードソロモン符号に基づく(k, n)しきい値法の秘密分散は，n 個のシェアのうち，$k - 1$ 個のシェアを保護対象の秘密情報に依存しないように設定できるという性質を有することに着目し，非正規の盗聴端末への情報漏えいの抑制を実現する．物理層のセキュリティにベクトルコーディングと呼ばれる信号処理を適用し，通信路のマルチパスの影響を考慮しつつ，複数送受信アンテナ伝送に限定されない，単一，及び，複数の送受信アンテナ伝送における情報漏えいの抑制を実現する．さらに，これらのふたつのセキュリティ技術を無線パケット通信に適用し，情報保護の特性を解析，及び，計算機シミュレーションにより評価する，以上を研究の方法とする．

４．研究成果

組織リードソロモン符号に基づく(k, n)しきい値法の秘密分散では，保護対象の秘密鍵から生成した n 個のシェア $v(0), v(1), \dots, v(n\text{-}1)$ のうち，$k - 1$ 個のシェア $v(0), v(1), \dots, v(n\text{-}2)$ は，秘密鍵に依存しないように設定できるという性質を利用し，これらのシェアのうちの m 個 $(m < k)$ を送信者と正規の端末の間で事前共有し，事前共有したシェアの送信は不要とすることにより，非正規の盗聴端末への情報漏えいを抑制する秘密分散方式を開発した．

構成例をもとに方式を説明する．図１は，組織 $(7, 3)$リードソロモン符号における情報シンボル (Information symbols)，パリティシンボル(Parity symbols)，符号語 (Codeword)を示している．独立な乱数を r_1, r_2，秘密情報を s とする．互いに異なる７個のシンボル $x_0, x_1, \dots, x_6 \in \{1, 2, \dots, 7\}$ に対して，２次多項式 $f(x)$ を，$f(x_6) = r_2, f(x_5) = r_1, f(x_4) = r_2 + r_1 + s$ となるように設定する．７個のシンボル $f(x_6), f(x_5), \dots, f(x_0)$ が符号語を構成する．$(7, 3)$リードソロモン符号は最小距離が４であり，符号語の少なくとも３個のシンボルを取得すると，符号語の７個のシンボルを完全に再生する．このとき，$s = f(x_4) - f(x_5) - f(x_6)$ により，秘密情報を s を再生する．７個の符号語シンボルを７個のシェアとすると，$(3, 7)$しきい値法の秘密分散を構成できる．しかしながらこのとき，正規の端末と非正規の盗聴端末において，秘密情報の再生条件は同一となる．

$v(0) = f(x_6), v(1) = f(x_5), v(2) = f(x_4), v(3) = f(x_3)$ として，４個のシェアを用いた$(3, 4)$しきい値法を構成すると，４個のシェアのうち，少なくとも任意の３個の取得が，秘密情報の再生条件となる．４個のシェアのうち，$v(0), v(1)$ は，秘密情報 s に依存しないため，固定値として，基地局と正規の端末の間で，事前共有が可能となる．従って，s の更新に伴って変化する $v(2), v(3)$ のみを基地局から端末に送信することになる．このとき，正規の端末は，$v(2), v(3)$ のうち，任意の１個を取得すると，s を再生する．一方，盗聴端末は，$v(2), v(3)$ の両方を取得しても s の再生は不可能で，盗聴端末への情報漏えいが抑制される．

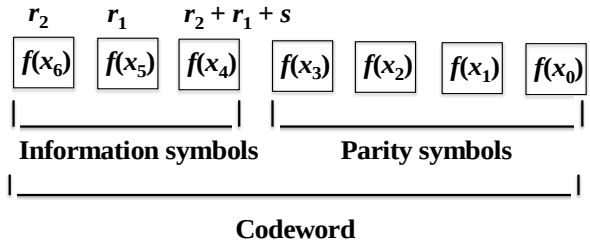

図１．組織(7, 3)リードソロモン符号を用いた(3, 7)しきい値法の秘密分散の構成

図２に示す基地局(Base station) から正規の目標端末 (Target terminal) への無線情報伝送において，通信エリア内に非正規の盗聴端末 (Eavesdropper terminal) が存在する系を無線通信系として想定し，基地局の送信機と目標端末の受信機の間で，ベクトルコーディングに基づくマルチパスを考慮した通信路行列 (Channel matrix)の分解により，単一の送受信アンテナ，及び，複数の送受信アンテナの両者の物理層のセキュリティに適用される伝送方式を開発した．

図３は，基地局が６個の送信シンボル $x_0, x_1, \ldots, x_5$ を送信し，正規の目標端末がそれらを６個の受信シンボル $y_0, y_1, \ldots, y_5$ として受信する構成例である．２個の送信アンテナ(T_0, T_1)，２個の受信アンテナ(R_0, R_1)を用い，各々のアンテナ間の通信路を $Channel_{0,0}$, $Channel_{0,1}$, $Channel_{1,0}$, $Channel_{1,1}$，そして，６個の受信信号に付加される加法白色雑音を各々，$w_{0,0}, w_{0,1}, w_{0,2}, w_{1,0}, w_{1,1}, w_{1,2}$ とする．このとき，送受信アンテナ間の通信路行列を H とし，H を対角化するときに生成される行列を P とすると，これらの行列を用いた基地局の前処理と目標端末の後処理により，目標端末では無干渉で送信シンボルが受信される．一方，非正規の盗聴端末では，基地局と盗聴端末間の通信路行列を G とするとき，$G = H$ でない限り，盗聴端末の受信シンボルは干渉を含み，情報の再生が困難となり，本伝送系は物理層のセキュリティとして動作する．

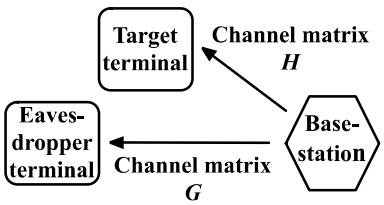

図２　想定する無線通信系の構成

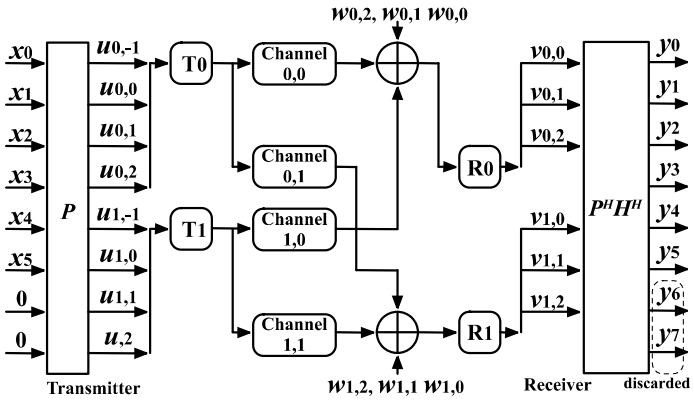

図３　物理層のセキュリティに適用されるベクトルコーディングを用いた伝送方式

基地局から端末への無線パケット通信において，ペイロードに収容される情報を暗号化する際の秘密鍵を組織リードソロモン符号に基づく(k, n)しきい値法の秘密分散を用いて n 個のシェア $v(0), v(1), \ldots, v(n\text{-}1)$ に分散する．このうち，h 個のシェア ($h \leqq n$)を，h 個のパケットのヘッダに収容し，端末にシェアを配信する通信方式を開発した．秘密分散のパラメータ設定に対応して，(1) 正規の端末が秘密鍵を再構成するために必要な受信シェア数の条件，(2) 非正規の盗聴端末が秘密鍵を再構成するために必要な受信シェア数の条件の(1)と(2)に応じた単一送受信アンテナ，及び，複数送受信アンテナの物理層のセキュリティの要求条件を導出した．

例えば，送信者と正規の端末の間で事前共有するシェアの数を $m = k - 1$ とし，かつ，基地局が正規の端末に向けて送出する事前共有していないシェアの数を $h = k - 1$ とすると，非正規の盗聴端末は，基地局から送出された $k - 1$ 個のシェアを全て取得しても秘密鍵の再構成は不可能であり，一方，正規の端末は，基地局から送出された $k - 1$ 個のシェアのうち，1 個を取得すれば秘密鍵の再構成がなされる．この場合は，物理層のセキュリティの適用は不要となる．

非組織リードソロモン符号に基づく(k, n)しきい値法の秘密分散を用いると物理層のセキュリティの適用が必要となる．この場合，計算機シミュレーションにより，正規端末，非正規端末の各々における秘密鍵の再構成確率特性を評価し，提案する物理層のセキュリティ方式の有効性を確認した．計算機シミュレーション評価結果の一例を図４に示す．16-QAM (Quadrature Amplitude Modulation)の変調方式で，２送受信アンテナ(L2)，３送受信アンテナ(L3)伝送を行い，各々の送受信アンテナ間の通信路は，パス数 $N = 2$ のマルチパス特性をもち，パスの利得は１個のパス毎に，$\beta = 60$ [dB] 減衰すると仮定している．非組織リードソロモン符号を用いた(8, 16)しきい値法の秘密分散により 16 個のシェアを生成し，16 パケットがひとつの伝送系列となる．秘密情報は 16 パケット毎に更新される．正規の目標端末(autho)，非正規の盗聴端末(unautho)は，各々，秘密情報の再生には，16 個のシェアにうち，少なくとも，8 個のシェアが必要となる．計算機シミュレーションでは，各種の受信信号対雑音比 (SNR) のもとで，シェアを受信することによる秘密情報の再生を，理論的なエントロピーの最大値で正規化したエントロピー(entropy)で評価している．entropy = 1 は，秘密情報が全く特定されないことを意味し，entropy = 0 は，秘密情報が完全に特定されることを意味する．図４から，非正規端末は秘密情報を特定不能であることが確認された．

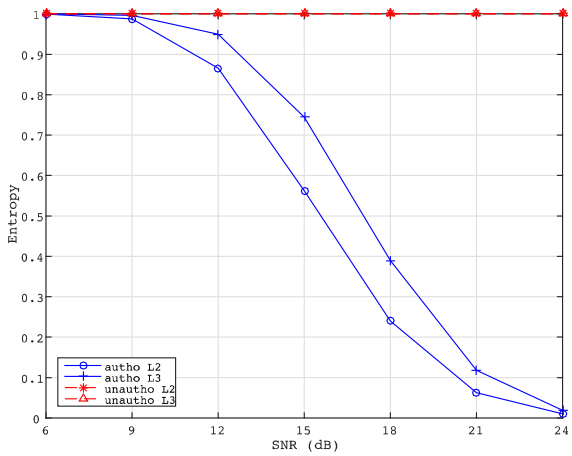

図４　計算機シミュレーションによる受信 SNR と情報再生の Entropy の評価結果

研究成果の主要な部分は，電子情報通信学会の雑誌論文④で提案され，研究成果は，同学会からの依頼による解説論文である雑誌論文②に周辺技術を含めて記載されており，さらに，同学会からの依頼による招待講演である学会発表③にも記載されている．

５．主な発表論文等

〔雑誌論文〕（計 6 件）

① 大村 光德, 宮崎 真一郎, 松嶋 智子, 山嵜 彰一郎, ``NFC を用いた ElGamal 暗号しきい値復号システムの開発,” 技能科学研究，査読有，印刷中, 2019.
② 山嵜 彰一郎, 松嶋 智子, ``[解説論文] 秘密分散と物理層の信号処理を用いた無線通信の情報保護方式,” IEICE Fundamentals Review, 査読有，Vol.12, No.2, pp.107-114, 2018.
③ 河本 椋，中村 信也，松嶋 智子，宮崎 真一郎，大村 光德，山嵜 彰一郎, ``拡張プライム系列符号と EWO 干渉除去方式を用いた可視光 CDM 伝送実験システム,”技能科学研究, 査読有，34 巻 1 号 pp.94-103, 2018.
④ Shoichiro Yamasaki, Tomoko K. Matsushima, Shinichiro Miyazaki, Kotoku Omura, Hirokazu Tanaka, ``Wireless Packet Communications Protected by Secret Sharing and Vector Coding,” IEICE Transactions on Fundamental Electronics, Communications and Computer Sciences, 査読有，Vol.E100-A, No.12, pp.2680-2690, 2017.
⑤ Tomoko K. Matsushima, Masaki Kakuyama, Yuya Murata, Yasuaki Teramachi, Shoichiro Yamasaki, ``A Study on Multi-User Interference Cancellers for Synchronous Optical CDMA Systems - Decision Distance and Bit Error Rate -,” IEICE Transactions on Fundamental Electronics, Communications and Computer Sciences, 査読有，E100-A, No.10, pp.2135-2145, 2017.
⑥ 宮崎 真一郎，山嵜 彰一郎，松嶋 智子，大村 光德, ``Overlap FDE を用いたシングルキャリア伝送の性能評価,” 職業能力開発研究誌, 査読有，33 巻 1 号, pp.76-81, 2017.

〔学会発表〕（計 13 件）

① 小野 恭平, 山嵜 彰一郎, 松嶋 智子, 宮崎 真一郎, 大村 光德, ``秘密分散と伝送系の信号処理によりセキュリティを強化した無線通信方式,” 電子情報通信学会 技術研究報告, WBS2018-123,pp.285-290, 2019.

② 河本 椋, 土居 勇人, 上村 健夢, 宮崎 真一郎, 大村 光德, 松嶋 智子, 山嵜 彰一郎, `` 拡張プライム系列符号を用いた可視光通信のための調光制御方式に関する一検討,” 電子情報通信学会 技術研究報告, WBS2018-98, pp.131-136, 2019.

③ 山嵜 彰一郎, 松嶋 智子, `` [招待講演] 秘密分散と物理層の信号処理により情報保護を強化した無線通信方式,” 電子情報通信学会 技術研究報告, IT2018-50, pp.85-90, 2019.

④ 河本 椋, 松嶋 智子, 宮崎 真一郎, 大村 光德, 山嵜 彰一郎, ``可視光 CDM 通信システムのための調光制御方式に関する研究,” 電子情報通信学会 技術研究報告, IT2018-41, pp.37-42, 2019.

⑤ 河本 椋, 土居 勇人, 上村 健夢, 松嶋 智子, 宮崎 真一郎, 大村 光德, 山嵜 彰一郎, `` 屋内照明機器のための調光制御可能な可視光 CDM 伝送実験システムの構築と評価,” 電子情報通信学会 技術研究報告, MICT2018-66, pp.31-36, 2019.

⑥ 河本 椋, 松嶋 智子, 宮崎 真一郎, 大村 光德, 山嵜 彰一郎, ``拡張プライム系列符号を用い可視光 CDM 通信のための調光制御方式の提案,” 電子情報通信学会 技術研究報告, WBS2018-23, pp.15-16, 2018.

⑦ 佐藤 紘樹, 芝 優志, 宮崎 真一郎, 大村 光德, 松嶋 智子, 山嵜 彰一郎, ``CDMA 無線通信における拡張プライム系列を用いた拡散符号の検討,” 第 40 回情報理論とその応用シンポジウム(SITA2017), 3.3.1, pp.148-153, 2017.

⑧ 芝 優志, 宮崎 真一郎, 大村 光德, 松嶋 智子, 山嵜 彰一郎, ``秘密分散を用いた分散ストレージシステムの信頼性を高める符号化方式の研究,” 第 40 回情報理論とその応用シンポジウム(SITA2017), 4.1.1, pp.174-178, 2017.

⑨ Tomoko K. Matsushima, Agus Susilo, Ryo Kawamoto, Shinichiro Miyazaki, Kotoku Omura, Shoichiro Yamasaki, ``A Study on Signature Codes and Bit Error Rate Performance of Synchronous Optical CDMA with MUI Cancellation,” 電子情報通信学会技術研究報告, WBS2017-31, pp.45-50, 2017.

⑩ 河本 椋, 中村 信也, 松嶋 智子, 宮崎 真一郎, 大村 光德, 山嵜 彰一郎, ``拡張プライム系列符号と干渉キャンセラを用いた可視光 CDM 伝送実験システムの開発,” 電子情報通信学会技術研究報告, WBS2017-23, pp.1-6, 2017.

⑪ 佐藤 紘樹, 芝 優志, 宮崎 真一郎, 大村 光德, 松嶋 智子, 山嵜 彰一郎, ``CDMA 無線通信における拡散符号の提案と多重ユーザ干渉除去方式の検討,” 電子情報通信学会技術研究報告, IT2017-19, pp.15-20, 2017.

⑫ 芝 優志, 宮崎 真一郎, 大村 光德, 松嶋 智子, 山嵜 彰一郎, ``分散ストレージシステムにおける秘密分散を用いた情報保護方式の研究,” 電子情報通信学会技術研究報告, IT2017-18, pp.11-14, 2017.

⑬ 山嵜 彰一郎, 松嶋 智子, 宮崎 真一郎, 大村 光德, 田中宏和, ``視覚復号型秘密分散の信号処理に関する研究,” 電子情報通信学会 2016 年ソサイエティ大会, 2016.

６．研究組織

(1) **研究分担者**

研究分担者氏名：松嶋　智子

ローマ字氏名：(MATSUSHIMA, tomoko)

所属研究機関名：独立行政法人高齢･障害･求職者雇用支援機構職業能力開発総合大学校**（能力開発院、基盤整備センター）**

部局名：能力開発院

職名：教授

研究者番号（8 桁）：30648902

(2) **研究分担者**

研究分担者氏名：宮崎　真一郎

ローマ字氏名：(MIYAZAKI, shinichiro)

所属研究機関名：独立行政法人高齢･障害･求職者雇用支援機構職業能力開発総合大学校**（能力開発院、基盤整備センター）**

部局名：能力開発院

職名：准教授

研究者番号（8 桁）：40648937

(3) **研究分担者**

研究分担者氏名：大村　光徳

ローマ字氏名：(OMURA, kotoku)

所属研究機関名：独立行政法人高齢･障害･求職者雇用支援機構職業能力開発総合大学校**（能力開発院、基盤整備センター）**

部局名：能力開発院

職名：准教授

研究者番号（8 桁）：40725719