博士学位論文審査要旨

２０１０年１２月２１日

論 文 題 目： ディジタル移動通信における電波伝搬特性を用いた秘密鍵共有・秘密情報伝送に関する研究

学位申請者： 北野　隆康

審 査 委 員：

主　査： 同志社大学大学院工学研究科　教授　　笹岡　秀一

副　査： 大阪大学大学院工学研究科　　教授　　三瓶　政一

副　査： 同志社大学大学院工学研究科　准教授　岩井　誠人

要　　旨：

陸上移動通信は、電波の傍受による盗聴の危険性があるため、その対策として暗号技術が適用される。しかし、計算量的な安全性に基づく従来の暗号技術は、演算能力の向上や新アルゴリズムの発見によって安全性が低下する懸念があるとともに、移動無線端末において鍵管理・鍵配送や演算能力の制限が問題となる。一方、情報理論的な複雑性を根拠とする暗号技術として、電波伝搬特性に基づく秘密鍵共有や秘密情報伝送が提案されているが、その多くは理論的な基礎研究の段階に留まり、実用的な方式の検討は少ない。

本論文は、電波伝搬特性を用いた暗号・情報セキュリティ技術の多様な実現可能性に着目し、その実現法の原理を示すとともに、実用の無線通信システムに準拠した具体的な方式を提案し、計算機シミュレーションによりその有効性を明らかにしている。ここで対象とした技術は、伝送品質に基づく秘密鍵共有方式、無線信号遮蔽による通信秘匿方式、干渉信号制御を用いた秘密情報伝送方式である。以下、本論文の内容の概要を説明する。

本論文では、はじめに研究背景を述べた後、電波伝搬の可逆性と場所依存性に基づく電波を用いた情報セキュリティ技術の基本原理を説明し、研究目的を示している。次に、電波伝搬特性に基づく秘密鍵共有方式を対象に、既存方式の異なる観測量を用いた新方式を検討し、擬似ビット誤りに基づく秘密鍵共有方式を提案している。提案方式では、受信機の復調機能を活用して、鍵共有に適した擬似ビット誤りを発生させる工夫を行っている。また、計算機シミュレーションにより無線 LAN 環境における提案方式の有効性を確認している。

次に、電波伝搬特性を用いた通信秘匿の実現可能性に着目し、先行研究がほとんどない無線信号遮蔽による通信秘匿方式を新たに提案した。この方式は、秘密情報を通常情報（カバー情報）で覆い隠すステガノグラフィの概念を無線信号に拡張し、無線秘密信号を無線カバー信号で遮蔽して秘密情報伝送の存在自体を秘匿するものである。提案方式では、既存のステガノグラフィと異なる新たな課題・問題を創意工夫により解決している。また、シングルキャリア伝送とマルチキャリア伝送の二つの実用的なシステムを対象として、計算機シミュレーションにより伝送品質と安全性に関する諸特性を評価し、提案方式の実用性と有効性を確認している。

次に、電波伝搬特性を用いた秘密情報伝送方式を対象に、より効率的で実用的な方式の検討を行い、複数アンテナからの干渉信号送信を用いた秘密情報伝送方式を提案している。この方式は、盗聴局に干渉を与える一方、正規受信局で干渉が打消すように送信制御を行うことで、秘密情報伝送を実現するものである。提案方式では、盗聴局の位置により干渉波が打消される場合に安全性が損なわれる対策として、干渉信号の送信重み制御を時間的に変動させる手法を採用している。

また、計算機シミュレーションにより提案方式の有効性を確認している。さらに、提案方式の手法を拡張して、実用化されているMIMOシステムへの適用を検討し、MIMO固有ビーム空間分割多重伝送に基づく秘密伝送方式を提案している。提案方式では、直交化された複数チャネルの一方を秘密情報伝送に、他方を秘密性の確保のための干渉信号伝送に用いている。また、計算機シミュレーションにより提案方式の実用性と有効性を確認している。

以上の結果から、論文提出者が提案した方式は、電波伝搬を活用した情報セキュリティ技術に関する先駆的かつ実用的な研究であり、この研究成果は、今後のこの分野の発展に大きく貢献することが期待される非常に価値の高いものである。よって、本論文は、博士（工学）（同志社大学）の学位論文として十分な価値を有するものと認められる。

総合試験結果の要旨

２０１０年１２月２１日

論 文 題 目： ディジタル移動通信における電波伝搬特性を用いた秘密鍵共有・秘密情報伝送に関する研究

学位申請者： 北野　隆康

審 査 委 員：

主　査： 同志社大学大学院工学研究科　教授　笹岡　秀一

副　査： 大阪大学大学院工学研究科　　教授　三瓶　政一

副　査： 同志社大学大学院工学研究科　准教授　岩井　誠人

要　　旨：

本論文提出者は、本学大学院工学研究科電気工学専攻博士課程前期課程を 2008 年に修了後、2008 年 4 月より本学大学院工学研究科電気電子工学専攻博士課程後期課程に在学している。この間、各年度において優れた研究成果を挙げ、英語の語学試験に合格し、中国語についても十分な能力を有すると認定されている。また、本論文の主たる内容は、電子情報通信学会論文誌 Vol.J92-B No.1, Vol.J92-B No.9 で受理・掲載され、Vol.J94-B No.2 で受理・掲載予定（2011 年 2 月）であるなど、十分な評価を得ている。

2010 年 12 月 11 日午後 1 時 30 分から約 2 時間にわたり、提出論文に関する学術講演会（博士論文公聴会）が開かれ、種々の質疑討論が行われたが、提出者の説明により、十分な理解がえられた。さらに講演会の終了後、審査委員により論文に関する諸問題に関する口頭試問を実施した結果、提出者の十分な学力を確認することができた。

よって総合試験結果は合格であると認める。

博士学位論文要旨

論文題目：　ディジタル移動通信における電波伝搬特性を用いた秘密鍵共有・秘密情報伝送に関する研究

氏　　名：　北野　隆康

要　　旨：

近年の無線通信の普及に伴い，盗聴対策技術が重要となっている．盗聴対策としては，共通鍵暗号方式を用いて情報を暗号化して伝送することが一般的であるが，この方式は暗号化と復号に同じ秘密鍵を使用するため，送受信局の間で事前に秘密鍵を共有しておく必要がある．この鍵共有の過程において第三者に盗聴される危険性があり，安全な秘密鍵共有方法の確立が重要な課題となっている．現在は公開鍵暗号方式を用いて秘密鍵を共有する方法がよく用いられている．公開鍵暗号方式は，盗聴局での解読に膨大な計算量が必要になることを安全性の根拠としているが，正規の受信局で復号する場合にも多くの計算量が必要になるため，消費電力の観点で計算量に制限がある移動通信端末での使用には課題が残る．これに対して，電波伝搬特性に基づく秘密鍵共有方式や，電波伝搬特性を活用した秘密情報伝送方式による秘密鍵共有などが提案されている．これらは，電波伝搬の可逆性や電波伝搬の場所依存性といった特徴を活用し，特定の局同士で同じ秘密鍵を生成する，あるいは，暗号を用いることなく安全に情報伝送を行うことを目的とした技術である．本論文では，これらの電波伝搬特性を用いた秘密鍵共有・秘密情報伝送を実現する新しい方式について提案し，有効性を明らかにした．

なお，本論文は以下の6章から構成されている．

第1章は序論であり，研究背景や基本原理，目的などを述べている．基本原理として電波伝搬の特徴である電波伝搬の可逆性と場所依存性を記すとともに，無線通信における従来のセキュリティ技術についても言及している．

第2章では，電波伝搬特性に基づく擬似ビット誤り率を用いた秘密鍵共有方式を提案した．電波伝搬特性に基づく秘密鍵共有方式は，秘密鍵の共有を所望する正規局の間で信号の送受信と伝搬路特性の測定を互いに複数回数行い，得られた伝搬路特性を多値量子化して秘密鍵を生成するものである．この方式では，伝搬路特性が，電波伝搬の可逆性により正規局間で互いに高相関となるのに対して，盗聴局では電波伝搬の場所依存性により低相関になることを活用している．これにより，伝搬路特性を活用して秘密鍵を生成すると，正規局間でのみ秘密鍵の共有が可能となり，盗聴局では同じ秘密鍵を得ることが困難となる．この方式については，受信信号強度（RSSI: Received Signal Strength Indicator）に基づいて秘密鍵を生成するものが多く議論されている．しかし，支配的な電波が存在する環境では安全な秘密鍵の生成が困難になることや，RSSIには伝搬路における位相変動が含まれないなどの課題があった．そこで本論文では，秘密鍵生成の共有情報としてRSSI以外の情報である擬似ビット誤りを用いる方式を提案した．擬似ビット誤りを用いることで，伝搬路特性のその他の変動を含めて秘密鍵を生成することが可能になる．ただし，擬似ビット誤りの発生方法によっては秘密鍵生成に必要な擬似ビット誤りが得られない可能性があり，その発生方法が重要となった．そこで，秘密鍵生成の共有情報に適した擬似ビット誤りを調査したところ，伝搬路の歪み補償を活用して擬似ビッ

ト誤りを発生させる方法が効果的であることがわかった．この擬似ビット誤りを用いて秘密鍵を生成する方式についてシミュレーションを行ったところ，効果的に秘密鍵が共有できることが明らかになった．

第3章では，電波伝搬特性を活用した通信秘匿を提案した．これは，情報伝送を行う通常の変調信号（カバー信号）の裏で，別の秘密情報信号（埋込信号）の送受信を行うことで，伝送行為自体を秘匿する方式である．これに類似の技術としてディジタルステガノグラフィがあるが，これは画像や音声などディジタルで保存する際に劣化が前提となる媒体に対して，秘密情報をディジタルデータのまま埋め込むことで情報を秘匿する方式である．一方，第3章の提案方式は，秘密情報を変調した埋込信号を，通常の伝送信号であるカバー信号に変調信号の形で埋め込む方式である．変調信号の形で埋め込むことにより，情報の形式に制限がなくなるという利点があるが，変調信号であるカバー信号の再現が容易となってしまうため，盗聴局でもカバー信号が除去可能になることが問題になった．そこで第3章では，埋込信号に拡散処理を用い，さらに，埋込信号自体を雑音などと識別が困難になるような形にすることで秘匿する方法を提案した．ここではシングルキャリア伝送とマルチキャリア伝送を想定し，それぞれの伝送において通信秘匿が可能になることを明らかにした．

シングルキャリア伝送では，埋込信号に直接拡散処理を施してカバー信号に埋め込むという形態をとった．ただし，直接拡散信号をそのまま用いるだけでは雑音のような波形にはならないため，送信局で人為的に雑音を付加することで埋込信号を雑音に近づけるという手法を用いた．一方，マルチキャリア伝送では，カバー信号にOFDM（Orthogonal Frequency Division Multiplexing）信号を用い，埋込信号には周波数領域への拡散信号を用いた．周波数領域へ拡散した信号は，そのままでも雑音のような波形になる．しかし，この方式では，埋込信号の拡散方法や通常のOFDMなどに付加されるガードインターバルによって自己相関特性にピークが発生し，盗聴局でもそのピークを検出することで埋込信号を検出することが可能になるという問題があった．拡散に関しては，通常とは異なる変則的な拡散変調を行うことで自己相関のピークを抑圧した．一方，ガードインターバルに関しては，同期のタイミングをカバー信号と同じにした上で，埋込信号のガードインターバルにダミーのデータを使用することで自己相関のピークを抑圧した．本論文では，シングルキャリアとマルチキャリアの2つの埋め込み方式について，埋込信号の秘匿性と伝送情報の安全性の観点から評価した．埋込信号の秘匿性については，カバー信号のビット誤り率特性と埋込信号の信号点配置で評価した．これらの結果より，埋込信号を埋め込んだ場合でもカバー信号などに不自然さが見られず，埋込信号の秘匿が可能であることを確認した．一方，情報の安全性については，埋込信号のビット誤り率特性により評価した．これは，正規受信局では秘密情報の復調が可能であるのに対し，盗聴局では復調が不可能であるという結果になった．以上により，通信秘匿の実用性を明らかにした．

第4章と第5章では，複数アンテナシステムにおける秘密情報伝送の確立を目的としている．秘密情報伝送方式は，送信局と正規受信局の間の通信容量が，盗聴局の通信容量よりも大きくなる場合に情報伝送を行うと，暗号不要で安全な情報伝送が可能になるというものである．この技術に関する従来の研究は，理論的な実現可能性の言及に留まっているものが多く，具体的な実現手法を提案しているものは少ない．また，雑音などの自然現象を利用するだけでは実現が困難であることも報告されている．

第4章では，送信局が複数の送信アンテナを持ち，受信局は1本のアンテナを持つMISO（Multi-Input Single-Output）システムを想定した秘密情報伝送方式を提案した．この方式で

は，複数の送信アンテナから盗聴妨害用の干渉信号を送信することで盗聴を妨害し，秘密情報伝送を実現する．このとき，干渉信号に対して正規受信局で受信されないような制御を行うことで，正規受信局には影響せず盗聴局での受信のみを妨害することを可能にした．しかし，常に同じ制御をする場合に，正規の受信局以外の場所でも干渉信号の電力が小さくなる場所が存在し，盗聴対策として万全ではないことが問題になった．そこで，干渉信号の制御を時間的に変化させ，正規受信局以外で干渉信号が小さくなる場所を時間的に分散させるという手法を適用した．この制御により，正規受信局以外の場所では干渉信号によって受信を妨害されるようになり，秘密情報伝送が可能となった．提案方式について屋内環境を想定した伝搬モデルを用いてシミュレーションを行ったところ，条件付相互情報量の観点で盗聴が困難であるという結果が得られ，有効性を明らかすることができた．

第5章では，MIMO（Multi-Input Multi-Output）固有ビーム空間分割多重伝送を対象とした検討を行った．この伝送方式は，事前に送受信局の間で伝搬路情報を共有し伝搬路に応じた送信制御を行うという点において，電波伝搬特性と送信制御を活用した秘密情報伝送とは親和性が高い方式である．そこで，まず，一般的な固有ビーム空間分割多重伝送をそのまま用いる場合の安全性を評価した．この結果により，一般的な固有ビーム空間分割多重伝送では，盗聴局に現実的な優位性を持たせると情報の安全性が確保できなくなることが明らかになった．そこで，固有ビーム空間分割多重伝送の固有値の大きいパスで情報伝送を行い，固有値の小さいパスは盗聴妨害用途で使用することで秘密情報伝送が可能になる方式を提案した．なお，この方式でも，送信情報の安全性を十分に確保するためには，第4章のような時間的な送信制御が必要となった．以上の方式についてシミュレーションを行い，秘密情報伝送が可能であることを明らかにした．なお，第4章と第5章の提案方式は，ともに送信制御により秘密情報伝送を実現するものであり，受信局には特別なハードウェアを追加する必要がないという利点がある．

第6章では，以上の研究を総括した結論を記す．

本論文で提案した方式は，電波を用いた盗聴対策の基礎的かつ実用的研究であり，当分野における今後の発展に寄与することが期待される．