博士学位論文審査要旨

２００７年8月２８日

論 文 題 目：　陸上移動通信における伝搬路特性に基づく秘密鍵共有・暗号化方式の研究
学位申請者：　北浦　明人
審 査 委 員：
　主　査：　工学研究科　教授　　笹岡　秀一
　副　査：　工学研究科　教授　　辻　幹男
　副　査：　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、その対策として一般に共通鍵暗号方式が適用される。しかし、これらの計算量的な安全性に基づく方式は、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、陸上移動通信において鍵管理や鍵配送が特に問題となる。一方、情報理論的な複雑性を根拠とする技術は、優れた特長を持つものの、その大半が理論的な検討に終始している。その中でわずかに電波伝搬特性を活用した暗号技術は、多少実現可能性の高いものであるが、基礎研究の段階に留まっている。

本論文は、電波伝搬路特性に基づく秘密鍵共有方式の実現可能性に着目し、基本的な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。以下に本論文の内容の概要を説明する。

本論文では、はじめに秘密鍵共有の原理と基本的な実現方式について述べている。その原理は、伝搬路特性の可逆性により正規ユーザ間で相関性の高い情報を共有する一方で、伝搬特性の不規則変動の場所・時間依存性により盗聴者による情報の取得を困難にするものである。また、基本的方式は、時分割復信による信号の送受、伝搬路特性の測定、測定値から鍵（鍵候補）への変換、鍵候補の不一致対策などの要素で構成される。

次に、より現実的で実用的な方式を目指すには、実用の無線通信システムへの適用が望ましいとの観点から、直交周波数多重（OFDM）方式、PHS 方式、超広帯域通信（UWB）方式を対象として、適用システムと動作環境に適した具体的な方式を検討している。

その結果、OFDM 方式に適用する場合には、平均化による測定精度向上、線形補間による測定時間差補償、誤り訂正による鍵不一致対策が必要なことを明らかにするとともに、通常の通信が行える回線状態（例えば、信号対雑音比 15dB）において、ほぼ 100%の鍵一致率が得られることを示している。また、OFDM 方式への周波数ホッピング（FH）干渉の除去のためには、メディアンフィルタの適用が有効なことを明らかにしている。

PHS 方式に適用する場合には、アンテナ切替えによる受信信号強度の大小比較から鍵生成を行うことが望ましいことを示すとともに、鍵不一致対策をより強化する必要性から誤り頻出ビット除去の適用を提案している。また、UWB 方式に適用する場合には、マルチパス伝搬の遅延時間差を用いる方法が優れていること、遅延波のサブピーク位置の検出誤りを多少許容する鍵不一致対策が必要なことを明らかにしている。

さらに、秘密鍵共有方式で問題であった「なりすまし」対策について検討し、提案した秘密鍵共有方式と認証方式との組合せ方式を提案し、その有効性を明らかにしている。

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暗号方式の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

２００７年8月２８日

論 文 題 目：　陸上移動通信における伝搬路特性に基づく秘密鍵共有・暗号化方式の研究

学位申請者：　北浦　明人

審 査 委 員：

主　査：　工学研究科　教授　笹岡　秀一

副　査：　工学研究科　教授　辻　幹男

副　査：　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 2005 年に修了後、2005 年 4 月より本学大学院工学研究科電気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、ドイツ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.J87-A No.10, Vol.J90-B No.3, VolJ90-A No.5 等に受理・掲載され、十分な評価を得ている。

2007 年 7 月 28 日午後 1 時から約 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：　陸上移動通信における伝搬路特性に基づく秘密鍵共有・暗号化方式の研究

氏　　名：　北浦　明人

要　　旨：

陸上移動通信などの無線通信においては，電波の傍受による盗聴の危険性があるため，その対策として計算量的な安全性に基づく暗号方式が一般に用いられている．一方，情報理論的な複雑性を安全性の根拠とする暗号技術があり，優れた特長を持つものの大半は理論的な検討に留まっている．後者に属するがより現実的な技術として，無線通信の伝搬路特性に基づく暗号技術が注目されている．しかし，それらは基礎的検討の段階であり，実用の無線通信システムへの適用を視野に入れた研究は行われていない．

本論文では，伝搬路特性に基づく秘密鍵共有方式について実用の無線通信システムへの適用を検討・提案し，計算機シミュレーションによりその提案方式の有効性を明らかにしている．ここで，無線通信システムとしては，用途・使用環境により広帯域陸上移動通信，狭帯域陸上移動通信，屋内高速無線通信を検討対象とし，それぞれの無線通信システムに適した秘密鍵共有方式を検討している．また，提案した秘密鍵共有方式の新しい応用として，認証技術への応用システムの検討を行っている．

広帯域陸上移動通信としては，周波数分割多重（OFDM：Orthogonal Frequency Division Multiplexing）通信方式が注目を集めている．このOFDM通信方式は，付加機能なしで広帯域の伝搬路情報が取得できる特徴があるため，本論文ではこの情報を共有情報として活用し，秘密鍵を生成する方式の検討を行っている．

狭帯域陸上移動通信としては，PHS通信を適用対象とした．PHS通信は，今やモバイルアクセスには欠かせない通信の一つとなっている．PHS通信では，OFDM方式のような広帯域の伝搬路情報を利用できないため，受信信号強度に着目し利用した．また，PHSの基地局は，通常，複数本のアンテナを備えているので，複数のアンテナの信号強度を活用した方式を検討した．

屋内高速無線通信として，今，注目されつつある超広帯域無線通信(UWB)を検討対象とした．この方式のおいては，超広帯域に渡って通信を行っているため，信号は非常に短いインパルス状になっている．このため，超高分解能を持った測距測位が可能であるため，本論文では直接波及び遅延波の到来時間差を活用する方式を検討した．

さらには，本論文では秘密鍵共有方式のみでは対処できなかった「なりすまし問題」を解決するため，秘密鍵共有方式を応用した認証技術についても提案を行っている．

本論文は，８章から構成されており，その構成内容は以下の通りである．

第１章は，序論であり，本研究の背景及びその目的について述べている．

第２章では，陸上移動通信への盗聴対策として，新たに提案を行う通信路の伝搬路特性を用いた秘密鍵共有方式の原理と陸上移動通信路の特性について説明を行っている．

第３章では，OFDM方式を対象とした秘密鍵共有方式を提案している。OFDM方式を用いた秘密鍵共有では、遅延プロファイルの測定が容易なCDMA方式を用いた秘密鍵共有と異なり、伝送路の周波数特性を直接に測定することが容易である。そのため、ここでは周波数特性に基づく秘密鍵生成法を採用している。また，提案方式の性能を評価するためにIEEE802.11aの無線LANの規格に準拠したモデルを用いて計算機シミュレーションを実施し，十分に良好な特性が

得られ実用システムとしての実現可能性を明らかにしている.

第４章では、OFDM 方式を用いた秘密鍵共有方式に対する干渉波の影響を検討している。第３章で提案したOFDM方式を用いた秘密鍵共有方式をIEEE802.11gの無線LANシステムに適用する場合，Bluetoothシステムが使用されていると、同一周波数帯域における干渉の結果、秘密鍵共有が極めて困難となる．そこで，本章ではBluetoothの規格に準じたFH干渉波が秘密鍵共有に及ぼす影響を調べ，その影響を軽減するフィルタの提案を行っている．計算機シミュレーションを行った結果，提案フィルタによる有効性を明らかにしている.

第５章では，PHS システムを対象としており、２値化処理として２つのアンテナの受信信号強度の大小比較を行うことにより秘密鍵を共有する方式を提案している．これまで，第３章，第４章で述べた秘密鍵共有方式では、しきい値による２値化処理を採用していたが、共有した秘密鍵に不一致が多く発生するために多くの対策を講じなければならなかった．そこで，本章ではしきい値による２値化処理を行わない秘密鍵共有方式の可能性を検討した。提案方式の性能を評価するために ARIB 標準規格の PHS をモデルとして計算機シミュレーションを実施し，SN 比15dBの現実的な設定環境下において秘密鍵共有が可能であることを明らかにしている.

第６章では，非常に短いインパルスを用いた超広帯域無線通信(UWB)方式に適した秘密鍵共有方式を検討している。UWB方式では、高いマルチパス分解能により遅延波の到来時間を精度よく測定可能であるので、遅延波の到来時間差に基づく秘密鍵生成法を採用している．また，その方式の有効性を計算機シミュレーションにより明らかにしている.

第７章では，無線伝搬路特性を基にした秘密鍵共有方式による無線LAN認証方式を提案している．無線LANは電波を利用しているため，盗聴やなりすまし等による情報漏洩・不正使用の危険性が有線LANよりも遥かに大きい．しかし，現在使用されている無線LAN認証方式は，以前から使われていた有線LANの認証方式を無線LANに応用したものであり，認証の処理は無線LAN機器で行うのではなく，有線LAN上に接続された認証用機器が別途必要となる．そのため，処理が複雑になるとともに，規模の大きな装置が必要となり，管理面・費用面でも負担が大きい．一方，移動通信の盗聴対策として，無線伝搬路特性に基づく秘密鍵共有方式が提案してきた．この方式は，移動通信伝搬路の相反性・可逆性を利用して秘密鍵を生成・共有するものであり，無線装置に小規模の付加回路を追加するだけで実現が可能な簡易方式である．それに従い，本章では，新たに認証用装置を必要としない簡易認証方式として，無線伝搬路特性を基にした秘密鍵共有方式による無線LAN認証方式の提案を行っている.

ここで，各章の関係を整理すると以下のようになる。第３章から第６章までで提案した秘密鍵共有方式は，秘密鍵を生成する通信環境によっても使い分けることができる．屋外での移動通信のように，移動速度が速くフェージング変動が激しい時には，短時間で独立性の高い伝搬路情報を共有でき，盗聴者と異なる十分な長さの秘密鍵を比較的容易に共有できるため，時変周波数特性に基づき秘密鍵を生成すると良い（第３，４章).

一方，フェージング変動が非常に緩やかな場合には，盗聴者に解読される危険性のある単調な鍵しか共有できないため，エスパアンテナなどを用いて人為的に伝搬路を変化させることが必要となる．このため，適用可能なシステムが限定され，装置規模も大きくなる．そこで，フェージング変動が比較的緩やかな場合には，エスパアンテナのような複雑な付加装置を必要としない簡易な方式として，アンテナ切換えにより伝搬路を変化させ，そのときの受信信号強度の大小比較に基づいて秘密鍵を共有する方式を採用すると良い（第５章).

さらに，室内等の近距離無線通信には，高いマルチパス分解能を持つUWB方式による秘密鍵共有方式を採用すると良い（第６章)．UWB 方式は時間幅の極めて短いインパルスを直接送信するため，受信信号が伝送路のインパルス応答そのものに近く，受信信号を観測することにより直接波と遅延波の到来時間差を容易に測定することができる.そのため，到来時間差を共有情報と

することで秘密鍵を生成・共有できる.

第７章の秘密鍵共有方式を用いた簡易認証方式は，各々の環境に応じた秘密鍵を生成した後，それぞれの環境で後に説明する認証の問題があるため，生成した秘密鍵を基に簡易認証を試みることとなる.

第８章は，以上の研究を総括した結論を記している.