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　６ 年　 ６ 月 ２４ 日現在

機関番号：１７１０４
研究種目：若手研究
研究期間：2019～2023
課題番号：１９Ｋ２０２７３

研究課題名（和文）無線通信における伝搬路特性を利用した物理層認証方式の開発

研究課題名（英文）Development of a physical layer authentication scheme based on propagation characteristics in wireless communications

研究代表者

廣瀬　幸（Hirose, Miyuki）

九州工業大学・大学院工学研究院・准教授

研究者番号：８０８０４５４１

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：秘密鍵暗号方式で利用される秘密鍵生成方法の開発において、伝送帯域幅、変調方式、送受信アンテナ数を考慮した実装が容易な鍵生成方法を理論的に検討し実験的に評価した。統計的アプローチにより様々な通信環境を想定することが可能となり、シミュレーションによる評価では、電波伝搬環境および伝送パラメータ（例えば、帯域幅や変調方式、アンテナ数）を変化させながら共有秘密鍵を計算し、その有効性を検証した。また変調方式の高度化や送受信アンテナの数を増やすことにより鍵生成の精度が向上することを確認した。そしてFPGAに開発した暗号方式を実装した通信機を用いて、複数環境で実験的に評価し理論と比較検討した。

研究成果の学術的意義や社会的意義
無線LANやBluetoothは市場が拡大し通信技術が発展しており、それとともに通信の安全性への要求が重要となる。物理層では通信の信頼性が重要であり安全性については余り議論されてこなかったが、本研究の成果により、秘密鍵生成方法に関する新しい視点が提供され、通信技術をセキュリティへ応用することで新たな安全性を確保の実用化に向けた重要な基盤が築かれました。

研究成果の概要（英文）：A theoretical investigation and experimental evaluation were conducted on key generation methods considering the transmission bandwidth, modulation scheme and number of transmitting and receiving antennas. The statistical approach permitted the assumption of various communication environments, and the effectiveness of the method was verified by calculating shared secret keys while varying the radio propagation environment and transmission parameters in a simulation-based evaluation. Furthermore, it was demonstrated that the accuracy of key generation is enhanced by increasing the sophistication of the modulation scheme and the number of transmitting and receiving antennas. The results were experimentally evaluated and compared with the theoretical predictions in several different environments, utilising a communication device with the developed cryptographic scheme implemented in an FPGA.

研究分野：情報セキュリティ

キーワード：物理層セキュリティ　電波伝搬　秘密鍵生成

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

超多数のセンサやデバイスにより構成される IoT ネットワークの進展とともに無線通信の利用も拡大している．ネットワークの接続台数の増加は， IP アドレスの管理の煩雑さや認証の負荷といった課題が生まれ，ユーザの負担が増えるとともにセキュリティの品質を下げている．

ネットワークセキュリティとして，IDS (Intrusion detection system) の設置，接続時のアクセス認証，TLS などにおける証明書認証，ファイアウォールなどレイヤやサービスなどによって様々なシステムが利用されている．無線 LAN のセキュリティである WPA2 はプロトコル仕様の脆弱性が報告された．さらに省電力効果のある通信規格として利用されている Bluetooth においては，DoS(Denial of Service)攻撃として BlueSmack や BlueBorne として脆弱性[CVE-2018-5383]など様々報告されている．

一方で新たなセキュリティである物理層に着目した認証技術として，秘密情報伝送・共有技術が検討されており，これは多重波環境の特性を利用した鍵共有技術で通信路の可逆性に基づいている．ある空間において同じ周波数で同じ時間に送信すれば，ある 2 地点における受信時の電波伝搬特性は，同一特性となる．このとき，異なる地点では干渉により異なる電波伝搬特性になり，ある 2 地点の電波伝搬特性を推定することは難しい．この特性を基に秘密鍵を生成することで鍵共有が可能となる．秘密鍵共有方式であることから簡易な回路で実現可能であり，鍵配送を必要としないので十分な安全性が実現できるという特徴がある．しかしながら，実装については課題であり，鍵の安全性の実験や具体的な実装方法について検討されているものがほとんどない．電波伝搬特性を利用するためには，そのメカニズムを知る必要がある．電波伝搬（通信路）の解析方法として絶対的手法と統計的手法に分けられるが，動的に変化するような環境では絶対的手法では演算処理量の多さから難しい．統計的手法で電波伝搬特性を得るためには実測定で得られた多数のデータをもとに解析する必要がある．そこで，無線 LAN および Bluetooth の通信規格を活用した秘密鍵生成方法および認証方式の開発を目指す．

２．研究の目的

このような背景において，WPA3 の発表やセキュリティパッチの配信など様々対策がとられているが，WPA3 を含め現行するネットワークおけるセキュリティ対策はデータリンク層以上である．物理層では通信の信頼性が重要であり安全性については余り議論されてこなかったが，通信技術をセキュリにティへ応用することで新たな安全性を確保できる．そこでユーザ不在にも対応できる簡易でセキュアな物理層における認証方式の開発を目的とし，特に本課題では，普及率の高い無線 LAN および Bluetooth において検討する．

３．研究の方法

無線 LAN は，伝送帯域幅および空間多重の拡大や変調多値数の増大による高速化，複数アンテナを利用した複数ユーザに対する空間分割多元接続により大容量通信を実現している．そこで，これら伝送帯域幅・変調方式・送受信アンテナ数を考慮し実装が容易な鍵生成方法を理論的に検討し開発した．受信信号はレイリー分布および仲上ーライス分布に従う屋内環境を想定し，占有帯域幅に配置された各信号が増減する状況を踏まえ，場所依存による鍵生成について検討した．この鍵は無線 LAN における暗号化方式で使用され，その生成方法は通信の安全性評価の指標の一つとなる．

さらに提案した鍵生成方式を用いて，屋内環境を模擬した伝送シミュレーションを実施した．このシミュレーションでは，電波伝搬環境および伝送の各パラメータを変化させることで共有秘密鍵を計算した．とくに伝送方式や帯域幅，什器や部屋の大きさ，材質といった送受信機の周辺環境の違いが，生成された秘密鍵の数や誤り率にどのような影響を与えるかを詳細に検討した．シミュレーションの結果，伝送方式や帯域幅，伝搬環境によって生成される秘密鍵の数や誤り率を環境パラメータに対して比較することにより，より多くの秘密鍵を生成できることが確認された．また変調方式の高度化や送受信アンテナの数を増やすことにより鍵生成の精度が向上することを確認した．そして FPGA に開発した暗号方式を実装した通信機を用いて，複数環境で実験的に評価し理論と比較検討した．また Bluetooth の通信方式である周波数ホッピング方式において，環境依存による安全性の評価について理論検討した．

４．研究成果

これまで理論ベースで議論されていた物理層セキュリティにおいて，開発した秘密鍵方式をFPGA に書き込み無線機に実装し評価することにより，実験的に評価が可能になった．開発方式を実装した無線機は，理論検討の範囲内であった従来の物理層セキュリティ技術と比較して，実験的な評価により秘密鍵方式の適用の可能性と，既存のセキュリティ対策に加えて新たなセキュリティ対策として，無線 LAN および Bluetooth 環境での攻撃耐性が実証された．また，セキュリティ強化が通信速度および信号の安定性が保持され通信の信頼性に与える影響がないことや，開発した秘密鍵方式を実装した認証システムはユーザ不在時にも適用可能な簡易認証方式として自動的に認証することを確認した．これにより，無線システムにおいて，ネットワーク層やデータリンク層では防ぎきれなかった偽アクセスポイントによる悪魔の双子攻撃や電波干渉などに対するセキュリティ対策として新たなアプローチを提示した．

本テーマある物理層セキュリティの研究は，国内外ともにセキュリティ分野では先進的な取り組みとして評価されている一方，秘密鍵方式に関しては理論検討の範囲内で議論されてきた．本研究開発の対象とした無線 LAN や Bluetooth などの普及率が高い通信技術であるとともに攻撃事例としても増加している，このような技術に対する実用化可能性として，物理層セキュリティ分野において通信技術の信頼性と安全性を同時に確保する新たな方向性として示唆した．

今後の展望としては，多端末ネットワークに耐え得るために秘密鍵数や精度評価を検討するとともに,他の無線通信技術への適用可能性を探る.また実環境でのフィールドテストを通じて、実用化に向けた具体的な課題を明らかにする予定である．

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 廣瀬　幸	４．巻 6
２．論文標題 電波を利用した無線通信技術の 新しい応用分野	５．発行年 2021年
３．雑誌名 明専会報	６．最初と最後の頁 11-12
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計4件（うち招待講演　2件／うち国際学会　1件）

１．発表者名 廣瀬幸
２．発表標題 無線LANにおける電波伝搬特性を利用した認証方式とその検討
３．学会等名 システム技術分科会（招待講演）
４．発表年 2022年

１．発表者名 廣瀬幸
２．発表標題 無線 LAN における電波伝搬特性を利用した認証方式
３．学会等名 電子情報通信学会　インターネットアーキテクチャ研究会（招待講演）
４．発表年 2021年

１．発表者名 廣瀬幸
２．発表標題 実践的演習を目的とした無線LANセキュリティ
３．学会等名 大学ICT推進協議会
４．発表年 2023年

１．発表者名 廣瀬幸
２．発表標題 Study of A Miniaturized, Circularly Polarized Microstrip Patch Antenna
３．学会等名 International Practical Applications Seminar on Electrical Engineering and Computer Science（国際学会）
４．発表年 2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関