審 査 の 結 果 の 要 旨

氏　名　　牛 瀬

本論文は「 Study on Secrecy-Enhanced Data Transmission for Cooperative Relay Networks （協力中継ネットワークのための高秘匿データ伝送に関する研究）」と題し、盗聴者が存在する環境下において協力中継を用いてデータ伝送を行う際に、フェーディングや雑音等の無線チャネルの物理的特性を利用してその秘匿性を高める手法の提案と性能評価の研究を行ったものであり、全七章から構成されている。

第一章は「Introduction」であり、本研究で対象とする協力中継ネットワークを概観すると共に、無線チャネルの物理的特性を利用してその安全性を評価するために必要となる secrecy capacity の概念を紹介し、これが目標とする secrecy rate を超える確率である secrecy outage probability を最小化することが安全性評価の指標となることを示している。

第二章は「Two-User Cooperation Analysis under Eavesdropping Attack (盗聴攻撃下での二人のユーザの協力の解析)」と題し、二人のユーザが協力中継を行うインセンティブについての理論的検討を行っている。複数のユーザが協力中継を行うと、チャネル容量の観点からは有利となるので中継に参加するインセンティブが存在する。しかしながら効用関数として、受動的な盗聴者が存在しても安全な伝送が行える確率である secure transmission probability を用いると、協力中継を行うことによる効用関数の増加は未知であり秘匿性向上の観点からは協力中継を行うインセンティブはない。しかしながらここでは、協力を行うユーザが十分近傍に存在する場合には、直接伝送を行う場合よりも協力中継を行った方が secure transmission probability は常に増加するため協力中継を行うインセンティブが存在することを導いている。この理論的な導出においてはチャネルの独立性の仮定が必要となるが、端末間の距離が 5cm と小さい場合であっても、十分独立性が確保できることをソフトウエア無線を用いた実験によりあわせて示している。

第三章は「Multi-User OUCS with Full Secrecy Diversity for Cooperative Relay Networks (協力中継ネットワークにおける複数ユーザによる OUCS を用いた匿名性確保)」と題し、協力中継を行うユーザが送信者の周辺に複数存在する場合に、どのようにして最適なユーザを選択すべきか、あるいは協力中継を行わないかをソースと各ユーザおよび盗聴者の間の CSI (channel state information)を利用して判断する手法について論じている。そのためにまず SPC (secrecy-providing capacity)と名付けた指標を定義し、最も SPC が大きいノードを中継ノードとすれば最小の secrecy outage probability が得られることを示した。次に解析的手法及びシミュレーションにより、盗聴者へリンクの CSI が未知な場合及び既知の場合のいずれであっても本手法が既存手法に比べ良好な特性を示すことを明らかにした。

第四章は「Secure Transmission through Cooperative Relaying in Wireless Body Area Networks (協力中継を用いた無線ボディエリアネットワークにおける安全な伝送)」と題し、第二章及び第三章で提案した手法の WBAN (wireless body area network)への適用について論じている。WBAN の場合、体内での信号減衰が自由空間より大きいためチャネル容量を増加する意味でも協力中継の適用は有望である。WBAN においてはフェーディング特性として、自由空間のようにレイリーフェーディングは仮定できないため、より現実的な仮定である log-normal フェーディングを用いて、これらの手法の解析的及びシミュレーションによる性能評価を行い、WBAN においてもこれらが利用可能であることを示した。あわせて中継ノードの最適配置につい

ても検討を行い、センサとゲートウエイノードの中間付近に中継ノードを配置することが secrecy outage probability の観点から最適であることを示した。

第五章は「Fountain Code Assisted Security for Internal Eavesdropping in CRNs with an Untrusted Relay (協力中継ネットワークにおける信頼できない中継ノードがいる場合のファウンテン符号を用いたセキュリティ)」と題し、中継ノード自身が盗聴者である場合の秘匿性向上のために fountain code を用いる方式である FCAS (Fountain Code Assisted Security)の提案を行っている。FCAS は、受信者が元データを復元に必要なパケットを受信した時点で、その後の冗長な中継を打ち切ることにより、盗聴者がデータ復元に必要な数のパケットを受信することを阻止する方式である。また、盗聴者がデータ復元できない確率を新たな秘匿性の評価指標としている。更にこの確率を高めるためには送受信者間のリンクのチャネル容量を一定以上に保つ送信電力と併用することが有効であることを解析及びシミュレーションにより示している。

第六章は「Fixed Linear Code Assisted Security for Resisting Multiple Untrusted Relays(複数の信頼できない中継ノードがいる場合の固定線型符号を用いたセキュリティ)」と題し、第五章と同じく、中継ノード自身が盗聴者である場合の秘匿性向上のために線形符号を用いる方式である FLCAS (Fixed Linear Code Assisted Security)の提案を行っている。FCAS には盗聴者が十分な数のパケットを受信できなくても一部分のパケットは復元できるという弱点があったが、FLCAS では一つのブロックを構成する全てのパケットが受信できなければ、部分的にパケットを復元することも不可能となるので安全性はより高くなる。但し FCAS のような前方誤り訂正能力はないため別途 ARQ 等の再送制御を必要とする。本章では FLCAS の性能評価を解析及びシミュレーションによって行い、更に FCAS と FLCAS の両者をソフトウエア無線を用いて実装し、実環境での性能評価を行い両者の利害得失を論じている。

第七章は「Conclusion & Future Works (結論と今後の課題)」であり、論文の成果と今後の展開をまとめている。

以上これを要するに、本論文は外部盗聴者及び中継ノードが盗聴者である環境下において協力中継を用いてデータ伝送を行う際に、フェーディングや雑音等の無線チャネルの物理的特性を利用してその秘匿性を高める手法を提案し、理論的解析・シミュレーション・実証実験を通じてその性能評価の研究を行ったものであり、電子情報学上貢献するところが少なくない。

よって本論文は博士（情報理工学）の学位論文として合格と認められる。