論文の内容の要旨
Abstract

論文題目　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）

氏　　名　牛　灝

Recent years have witnessed an explosive increase in the research works on cooperative relay networks (CRNs) to improve the reliability and efficiency of wireless data transmission at the physical layer. Unlike these works, this thesis focuses on secrecy-enhanced data transmission for CRNs at the physical layer from the perspective of physical layer security (PLS). There are generally two kinds of eavesdropping attacks for CRNs: external eavesdropping attack from pure eavesdroppers and internal eavesdropping attack from untrusted relays. The thesis is thus divided into two parts by considering these two kinds of attacks.

In the first part of the thesis, the cooperative relaying for protecting from the external eavesdropping attack, also named cooperative security, is studied. 1) We first investigate the cooperative security for the typical two-user cooperation scenario within the framework of game theory. Due to the fact that the conventional cooperation may deteriorate the secrecy performance compared to the direct transmission (DT), an opportunistic user cooperation scheme (OUCS) is designed. The OUCS activates the cooperation only when it is regarded to be worthwhile according to the time-varying channel fading. It is proved that the OUCS consistently achieves a better secrecy performance than the DT, which motivates the users to cooperate with each other. 2) Then, we extend the OUCS to multi-user cooperation scenarios by jointly solving the questions of whether to cooperate and with whom to cooperate under the eavesdropping attack. It is derived that the full secrecy diversity performance is realized by the OUCS, which outperforms existing alternatives in the literature. 3) Moreover, we consider the application of cooperative security in a kind of specific sensor networks - wireless body area networks (WBANs). Based on the channel characteristics of WBANs, the secrecy outage probabilities for the DT and cooperative relaying are derived respectively. It is confirmed that the cooperative security is also feasible in WBANs.

In the second part of the thesis, the code assisted security for protecting from the internal eavesdropping attack is investigated. Because the cooperative relays themselves are the eavesdroppers in this case, the cooperative security analyzed above is no longer effective. Therefore, the code assisted security is introduced. 1) We first design a scheme of fountain code assisted security (FCAS). Because the receivers need a sufficient number of fountain packets to recover the original data for fountain coded transmission, the security can be achieved if the destination receives fountain packets faster than the eavesdropper. The channel fading and transmit power control are exploited by us to make a higher packet reception rate at the destination compared to the eavesdropper. It is observed that FCAS reduces the intercept probability to zero (near-)exponentially with increased number of source packets. Therefore, an arbitrarily small intercept probability can be realized by simply increasing the number of source packets. The conclusion is also held when we apply FCAS in the CRNs to resist an untrusted relay. 2) We further develop a fixed linear code assisted security (FLCAS) scheme based on FCAS, and use it to resist multiple untrusted relays. Because the randomness characteristics of fountain codes still results in a small quantity of data leakage, we are motivated to adopt a fixed linear code with a better secrecy performance. The intercept probability for FLCAS in the CRNs with multiple untrusted relays is then analyzed. It is found that FLCAS maintains the superiority of FCAS that the intercept probability is decreased to zero exponentially as the number of source packets increases. The destination based jamming strategy is also considered to accelerate the rate of decrease. In addition, the comparisons of FLCAS with FCAS and experiment evaluations are presented.

Overall, this thesis comprehensively studies how to enhance the secrecy of data transmission for the CRNs based on the concept of PLS. Both of the external and internal eavesdropping attacks are considered. The contributions herein can be also applied in the conventional multi-hop networks to improve the data transmission security.