**INVESTIGATION ON SECURE BEAMFORMING IN MIMO-NOMA BASED COGNITIVE RADIO NETWORKS**

**ABSTRACT**

The Cognitive Radio Network (CRN) and Non-Orthogonal Multiple-Access (NOMA) is an important scheme in the 5G radio transmission system. Nevertheless, it's a special path for the cognitive users for the security of transmission among the cells from the interferences in the MIMO-NOMA based CRN framework. In the research work, a novel perturbation based beamforming method is suggested for the secure exchange between the cells from all other interfered users. There are four distinct techniques suggested in the research work along with the novel second-order perturbation beamforming technique to validate the security in the system model as follows: Maximum Ratio Transmission (MRT) scheme, Equal Power Splitting (EPS) along with the MRT technique, linear Minimum Mean Square Error (MMSE) scheme and low complexity iterative linear MMSE (i-MMSE) technique.

The interference is caused by the imperfect spectrum sensing of the SUs. The SUs are intended to access the primary users (PUs) channel. In the same time, the PU also comes back to the channel before the SUs access ends. Thus, the similar way of accessing the PU channel will cause interference among the users. Thus, the impact of interferences will be greatly reduced by the distinct techniques and the novel second-order perturbation scheme. Among them, the novel second-order perturbation technique will highly maximize the entire secrecy rate of the system in the MIMO-NOMA network strategy. The simulation analysis obtains better proof for the performance of the novel second-order perturbation beamforming technique. The distinct techniques and the novel second-order perturbation method in the research is simulated between the two cells in the system model. Because the minimum number of two cells in BS can also be stretched into multi cells easily.

The best method is acquired by comparing all the performance analysis of the distinct techniques and the novel second-order perturbation technique to obtain the

optimum method. The optimum method is furthermore validated by the asymptotic simulation in the performance analysis of the secrecy outage probability.

The simulation results give better proof for the enhancement of the novel second-order perturbation technique. The simulation performance analysis contains throughput, secrecy rate, Bit Error Rate (BER), capacity of the channel, Secrecy Outage Probability (SOP) analysis and the analysis of ergodic secrecy capacity of the system. The novel second-order perturbation contribution has the power restriction mechanisms in the transmitted antennas during the data exchange among the cells.

The four techniques and the novel second-order perturbation performance are executed perfectly in the research task. This task efficiently secures the system model in the research field, and also do not withdraw their efficiency in the other research area. Therefore, from all these performances, one can declare that the above novel second-order perturbation technique is much utilized to enhance the security of the system. This prompts the research task to employ the technique to accomplish the research destination as soon as possible. One can apply the research work for the best precise communication in the MIMO-NOMA based CRN system framework, without causing any intervention.