

**CHENNAI – PONDICHERRY**

**FTP-NDN File Transfer Protocol Based on Re-Encryption for Named Data Network Supporting Nondesignated Receivers**

**Abstract**

Due to users' network flow requirement and usage amount nowadays, TCP/IP networks may face various problems. For one, users of video services may access simultaneously the same content, which leads to the host incurring extra costs. Second, although nearby nodes may have the file that a user wants to access, the user cannot directly verify the file itself. This issue will lead the user to connect to a remote host rather than the nearby nodes and causes the network traffic to greatly increase. Therefore, the named data network (NDN), which is based on data itself, was brought about to deal with the aforementioned problems. In NDN, all users can access a file from the nearby nodes, and they can directly verify the file themselves rather than the specific host who holds the file. However, NDN still has no complete standard and secure file transfer protocol to support the ciphertext transmission and the problem of the unknown potential receivers. The straightforward solution is that a sender uses the receiver's public key to encrypt a file before she/he sends the file to NDN nodes. However, it will limit the behavior of users and incur significant storage costs of NDN nodes. This paper presents a complete secure file transfer protocol, which combines the data re-encryption, satisfies the requirement of secure ciphertext transmission, solves the problem of the unknown potential receivers, and saves the significant storage costs of NDN nodes. The proposed protocol is the first one that achieves data confidentiality and solves the problem of the unknown potential receivers in NDN. Finally, we also provide formal security models and proofs for the proposed FTP-NDN.