

**CHENNAI – PONDICHERRY**

**A NETWORK CODING AND DES BASED DYNAMIC ENCRYPTION SCHEME FOR MOVING TARGET DEFENSE**

**ABSTRACT:**

Unlike prior efforts in cybersecurity research, a dynamic defense theory, called moving target defense, increases the complexity and costs for attacks by effectively restricting the vulnerability exposure and the attack opportunities through various continually-changing evaluation, development mechanisms and strategy. Data encryption standard (DES) was the classical scheme of the traditional symmetrickey encryption schemes. Now it has been gradually replaced by the triple DES or advanced encryption standard (AES) so that the encoder has a larger key space. However, both the triple DES and AES cannot meet the dynamic security requirements of dynamic defense due to their static extension to the key space. In this paper, we propose a dynamic three-layer encryption scheme based on DES and network coding, with a low-complexity partial key update mechanism. Based on the theoretical analysis, the new scheme is shown to have the benefit to achieve a dynamic transition between efficiency and security, which increases its adaptability to various cyber conditions. The simulation results also show that the running ratio of the new scheme is relatively lower than or comparable to the triple DES.