Host Identity Protocols (HIP) is entirely new protocol proposed to compensate for increasing security issues in the current Internet architecture. HIP uses secure Diffie-Hellman (DH) cryptographic key exchange authentication system. DH works on one way encryption that is difficult to decrypt. One way encryption is based on exponential functions that are not easy to reverse. Implementation of HIP in the current Internet architecture requires HIP proxy server. Capabilities of proxy server include translation of HIP on Internet. The current OSI network model depends on IP addresses namespace. In IP networks the locator part of the IP address change if the host moves, effecting the upper layers of the network model. HIP isolates this problem by assigning a new fixed identity to the host.

The thesis provides coherent study of Host Identity Protocol Proxy and demonstrates the working of these systems under SystemC platform. The results corroborate the implementation of Host Identity Protocol in an embedded environment through simulations. The study also discusses several development scenarios of Host Identity Protocol enabled network. Consequently two designs of an HIP base exchange between two HIP enabled hosts are simulated. The design follows two logics, a combinational logic and a synchronous logic. The simulations performed during the study open opportunities which may help for the application of HIP in hardware environment. The findings of the present study applied appropriately may result technological advancement in network security systems.

Keywords: Host Identity Protocol, HIP Proxy, Network Security, Diffie-Hellman, Internet Protocol