Hybrid RSA-AES Encryption Algorithm for Securing Information Centric Networking (ICN) Model

Thathan Sureshkumar, Mani Lingaraj and Bojan Anand

Abstract---Information Centric Networking (ICN) is an evolving approach in the wide area of networking which offers promising solutions to existing problems in the network architectures. Many kinds of architecture solve the problem of centric networking but the verification in end-to-end security is not provided trustworthily. Transport layer security allows encrypted communication between two mediums that ensures absence of third party involvement while exchanging data in the connection with server. When adapting Transport Layer Security (TLS) for ICN the security of the end-to-end process becomes an overhead which doesn't provide a verification process for the type of user. To address the issue of user verification, Hybrid Rivest Shamir Adleman-Advanced Encryption Standard (HRSA-AES) algorithm is proposed in the transport layer. RSA produces a secure key 1 and AES also produces a secure key 2. Finally HRSA-AES, hybrid secured key is created by combining the secure key 1 and secure key 2 which is used to provide end-to-end user security verification in ICN. HRSA-AES algorithm provides the verification of the public key and private key which is utilized by the user. ICN model is implemented in NS2 simulation tool and provides a higher level of security to the ICN model with lower time of transmission in end-to-end cryptographic verification. The results are compared to the existing ICN and middleboxs.

Keywords---Information Centric Networking (ICN), Middleboxes, Hybrid Rivest Shamir Adleman-Advanced Encryption Standard (HRSA-AES) Algorithm, Cryptography, Transport Layer Security (TLS), and Security.