147. SECURED DATA COMMUNICATION IN DISTRUPTION TOLERANT NETWORK FOR SELFISH AND MALICIOUS NODE

M. Bhavani (1), PG Scholar, Veltech University, Chennai. Tamil Nadu,
R. Srinivasan(2), Assistant Professor ,Department of CSE, Veltech University, Chennai. Tamil Nadu,
bhavani5018@gmail.com (1), srinivasanrajkumar28@gmail.com (2)

DTNs to deal with find out the malicious, selfish misbehaving nodes and genuine loss nodes. Selfishness is social selfishness, as very often humans carrying communication devices in a DTN are socially selfish to outsiders but unselfish to friends. Maliciousness refers to malicious nodes performing trust-related attacks to disrupt DTN operations built on trust. There is no Systematic Monitoring of Behavior of Nodes in DTN. Data Loss is more in such a kind of Network. In the proposed system we are Monitoring Nodes Behavior & we are detecting Normal, Selfish & Malicious Nodes so that an Alternative Best Route is chosen. Selfish Nodes are Harmless but it will Receive Data from their Friends List. Malicious Nodes will Drop/ Redirect Packets once they are attacked. Energy Level based data Transmission is achieved. We aim to design and validate dynamic trust management protocol for DTN routing. QoS trust: We consider "connectivity" and "energy" to measure the QoS trust level of a node. Social trust: We consider "healthiness" and social ''unselfishness" to measure the social trust level of a node. Packets are encrypted using RSA algorithm.

Index Terms: Distruption tolerant network, Dynamic trust management, algorithm, Selfish and malicious node.

ISBN 978-81-904760-6-5