Distributed Detection of Clone Attacks in Wireless Sensor Network Using Optimized RED Algorithm

C.Brindha[1], K.Sharmila benasir[2], A.R.Narendrakumar[3]

[#1, #2] U.G Student,[#3]Assistant Professor,Dept. of CSE, University College of Engineering-Thirukkuvalai, Anna University,T.N, India.

[#1]brindhashre@gmail.com,[#2]sharmibena420@gmail.com,[#3]narenchandran@yahoo.com

Abstract- One of the most sensitive problems in wireless sensor network security is the node Clone attack. In this attack, an adversary breaks into a sensor node, reprograms it, and inserts several copies of the node back into the sensor network. Cloning gives the adversary an easy way to build an army of malicious nodes that can cripple the sensor network. A few distributed solutions to address this fundamental problem have been recently proposed. However, these solutions are not satisfactory. Therefore, first, analyze the desirable properties of a distributed mechanism for the detection of node Clone attacks. Second, one shows that the self-healing, Randomized Efficient and Distributed (RED) protocol for the detection of node Clone attacks do not completely meet our requirement, finally should optimize the RED protocol by include the distributed hash table (DHT) and shows that it satisfies the introduced requirements.