IMPLEMENTATION OF LEACH PROTOCOL USING HOMOMORPHIC ENCRYPTION

ALISHA GUPTA[1] & VIVEK SHARMA[2]

[1]Research Scholar, JMIT, Radaur, Haryana, India

[2]Assistant Professor & H.O.D, JMIT, Radaur, Haryana, India

ABSTRACT

Encryption schemes that support operations over ciphertext are of utmost importance for wireless sensor networks & especially in LEACH protocol. The salient limit of LEACH is energy. Due to this limitation, it seems important to design a confidentiality scheme for WSN so that sensing data can be transmitted to the receiver securely and efficiently and at the same time energy consumed must be minimum. Hence we proposed LEACH_HE in which confidentiality scheme i.e. homomorphic encryption is added to LEACH protocol. In homomorphic encryption data can be aggregated algebraically without decryption and hence less energy consumption. Simulation results are obtained in terms of three metrics- total energy consumed, amount of data transmitted and number of nodes alive. It is observed that the performance of LEACH_HE is somewhat similar to LEACH.

KEYWORDS: Clustering, Homomorphic Encryption, LEACHl, LEACH_HE, Wireless Sensor Network (WSN)