# ***Secured Routing for Opportunistic Sensor Networks***

***Abstract:*** Sensor networks are the backbone of many real time applications with several advantages and creating mammoth opportunities. In current situation wireless sensor networks play a crucial role in daily life. Several paramount developments, such as IoT, smart cities, smart houses, forest monitoring, environment monitoring, and monitoring/detecting COVID-19 cases and so on are realized by sensor networks.

To realize an efficient data gathering process, an efficient clustering method has been presented using Range Based Clustering (RBC) algorithm. Here clustering is performed based on the range value of each sensor node and Cluster Head (CH) selection is carried out based on residual energy and distance with sink node. For secure data transmission two novel routing algorithms have been proposed, namely Path Protected Hop-by-Hop (PPHH) algorithm, and Minimum Waiting Time Routing (MWTR) algorithm. In PPHH algorithm, optimal path for transmission is selected based on reliability of path and the selected path is verified by security node to find the security level of that path. Through these processes PPHH algorithm selects reliable and secure path for transmission. MWTR algorithm selects transmission path based on Packet Reception Ratio (PRR) of each node which expresses the trust value of that node indirectly. MWTR selects the most trustworthy route for transmission based on the TV (trust value) of each node in the path.

To further improve security during data transmission this proposed work presented effective cryptography techniques. Based on security level requirement, three different cryptography techniques have been proposed in OSN based military application. Code-based cryptography which is an innovative and highly secured technique is incorporated for commando-commando communication, whereas conventional Hyper Elliptic Curve Cryptography (HECC) technique which provides fast encryption and decryption is involved in soldier-soldier communication. Novel Design-based cryptography technique is proposed to secure commando-soldier communication. Light weight Key Generation (LWKG) scheme provides a simple mechanism to generate and manage encryption key in OSN. Here each CH is provided with master key and data transmission between CH and sink node encrypted by symmetric key cryptography technique using master key. Thus this research work enables highly secured transmission in OSN by providing secure routing and security provisioning schemes. Experimental results show promising improvements in terms of throughput, packet delivery ratio, packet overhead, energy consumption, network reliability, detection ratio of replicas, and coalition attack resistance.

**MD SALMAN ARAFATH**