ABSTRACT

In Wireless communication, the term “Heterogeneity” refers to interoperability between various multi coverage protocols. It is mandatory to provide rapid automatic development in cross interaction networks. It may be considered as advanced technique of Multi hop networks. The heterogeneous network provides active environment like users can communicate with each other at any time any where through any media including instant messages, e-mail, voice and video.

Heterogeneous network consist number of participating nodes in different categories or classification. The node characteristics in these networks are diverging significantly from each other. These characteristics include Computational Power, Memory, Transceiver Strength, Operating Frequency, bandwidth and of Operating Power Supply modes. The migration from homogeneous to heterogeneous network architecture, to support broad range of connectivity and it makes more attention to the issues like network management, routing, handover, security and privacy etc.

Today’s distinctive heterogeneous network contains member nodes range from 8-bit microprocessor based tiny devices to 128-bit multi-core monster devices. An unusual fall in manufacturing cost of modern mobile devices caused increasing number of IoT (Internet of Things) nodes and smart mobile device participants in LTE (Long Term Evolution) networks. Each access networks have different mobility, QoS (Quality of Service) and security constraints. In cellular network, explosion of data traffic and increasing node density needed for increasing network capacity. Compared to 3G, the 3GPP and LTE offers higher data rate. The heterogeneous deployments significantly increase the capacity of LTE networks. The work groups IEEE 802.21 provide media independent handover function and work with per authentication scheme.

Heterogeneous network will make the demand of power utilization, bandwidth, security and other QoS aspects. The most dangerous attacks are Denial Of Service(DOS), Brute force attack(BFA), Shell Shock attack, Secured Socket attack, Back door, Botnet attack and black hole attacks. These attacks could be eliminated by using High intruding techniques which requires high computational and operating power. So the node with least power can be affected by the various attacks. Heterogeneous nodes are containing both low and high power nodes in the modern IoT devices. So the existing security protocols are vulnerable to the modern dynamic nature of network. Hence it makes the requirement of improvement in the security protocol design.

The proposed work consists of two modules. The first module exhibit the concept of Genetic algorithm based Bacterial Foraging Optimization, in which all the nodes in the network as a elements and it can be analyzed by the various processes of Genetic algorithm. In this, node's behavior is simulated to the Ecoli bacterium in genetic algorithm. For example, the node movement can be pretended as Ecoli bacterium which can move for certain period of time either by swimming in the same direction or tumbling in the another direction. The actual path of the node movement is tracked by the swimming or tumbling process of the bacteria. Spilling over is the process of Genetic Algorithm (GA) that is simulated to the concept of Clustering in the network. Finally by using this process of Genetic Algorithm based Bacterial Foraging Optimization (GABFO), it optimizes all the basic parameters by the periodical updates.

The second module exhibits the use of three pass protocol. As a result, the method used in the three pass protocol provides more security to the message transmission against the various networking attacks. This protocol uses the asymmetric encryption method for high protection. The sender and receiver use different keys for encryption and decryption. The existing security protocol like secured IPv4 and secured IPv6 provide high security to only supported nodes based on addressing scheme. The secured IPv6 provides security to the nodes connected with 128 bit addressing and the Secured IPv4 provides security

only for the nodes with 32bit addressing. Hence, heterogeneous architecture includes 8 bit for all type of nodes. So, the secured IPv6 does not provide high security to dynamic nature of nodes in the network.

In order to achieve better QoS in the heterogeneous wireless network, Genetic Algorithm based Bacterial Foraging Optimization with Three Pass Protocol Algorithms are Proposed. The GABFO procedure have been applied for clustering and routing concepts performed on the nodes in the heterogeneous network and this procedure combined with the Three-Pass Protocol (TPP) to perform the security aspects like to identify malicious nodes and isolates it from the communication network. Automatically it turns to increase the QoS factor such as throughput. The security strength measured in terms of percentage is a main advantage of this aspect. Therefore, the behaviors of the network are observed and calculate the average value for all QoS factors. Since the research is focus on IoT devices, security and power utilization is the important factor. The performances of the protocols are varied based on the number of cluster formation. The analysis shows the proposed GABFO with TPP which provides optimum performance compared to conventional protocols like IPv4, Secured IPv4, IPv6, Secured IPv6.Hence the proposed GABFO with TPP provides 97% of security, 98% throughput with 35% of power utilization. At the end, the research has proven GABFOTPP consumes less power and provides more security compared to an existing protocols.