ABSTRACT

The ultimate goal of the research work is to improve the security in the Wireless Mesh Networks (WMN) and also to provide the maximum throughput. Generally the Wireless Mesh Networks uses the hybrid routing protocols to handle the traffic flow in the Mesh network. But, the hybrid protocols did not consider the security related problems. The proposed research work aim to enhance the security at the same time provides the maximum throughput. The research is divides into four phases. They are,

- Cryptographic key predistribution scheme
- Refuge based privilege key distribution scheme
- Self seeking node detection scheme

The proposed routing protocol is Advanced Protective Ad-Hoc On demand Distance vector routing protocol which can securely discover the route between the pair of nodes in the Wireless Mesh Network. In first phase, we are utilizing Polynomial bivariate key predistribution scheme to provide authentication and security. In this scenario each node is assigned with random key as well as polynomial bivariate key. By using this, the link will be generated dynamically by analyzing the key values. The source node sends a hello message which contains the Source node ID. The node within its transmission range will compute the key value by evaluating each of its polynomial shares. After identify that both are having the same polynomial, the source node broadcast its random key. When the node within its communication range heard this message, it will compute the communication key which is used for authentication. Then route its data packets through this node.

Secure routing for wireless mesh networks has focused on metrics that estimate link quality to maximize throughput. In second phase, the novel method to provide security and maximum throughput is introduced. To route the data packets securely and also to provide high throughput in wireless mesh networks, we propose a novel method called as Refuge based privilege key distribution scheme. In this scheme, Each and every node present in the network is authenticated with each other by sending authentication request. The authentication key is generated by considering the
distance between the nodes and the energy of that node. While routing the data packets the source node forward the data only through the authenticated nodes. The authenticated next forwarder is selected by its key value as it considers the energy and the distance.

The wireless mesh network enables a cooperative communication between the nodes in the mesh topology. Each node in the mesh network serves as a relay nodes for other nodes. The cooperative communication in the wireless mesh network faces one challenge of relay node behaves as a self-seeking node. The self-seeking node never performs its functions for other nodes. The self-seeking node performs its own functions correctly but it never shares its resources and serves for other nodes. To handle such a problem, we propose a new methodology with the consideration of self-seeking nodes in third phase. The self-seeking node is detected by using the self-seeking detection algorithm. After that, the routing protocol never chooses the self-seeking node as the relay node. The performance of our proposed research methodology is analysed by using the Network Simulator (NS2).