ABSTRACT

A Mobile Ad-hoc Network (MANET) is a constantly self-configuring, infrastructure-less network which communicates with each other by forming a multi-hop network. The natural characteristics of MANET make them vulnerable to passive and active attacks, in which misbehaving nodes can eavesdrop or delete packets, modify packet contents. Strong identification mechanisms are needed as unauthorized entities occur in MANETS. Privacy and Reliability constraints get failed when malicious nodes access sensitive data.

The Enhanced Identity-Based Cryptography (EIBC) method concentrates on providing strong authentication and secure communication among nodes in MANET. The proposed work discuss about establishing a secure route among MANET using Improved Ad Hoc On-Demand Distance Vector (IAODV) routing protocol and to select a node as a Private Key Generator (PKG) in a network, which generates and distributes public and private keys to the nodes in the MANET.

In the proposed work PKG node is used instead of the Trusted Third Party (TTP) or Certificate Authority (CA) for generating and distributing keys. As MANETs are dynamic in nature, when PKG node leaves
the network, then MASTER-SLAVE technique is used to select another PKG node. When a network is established and a secure route is also identified, communication is done using multi-mode routing algorithm based on the count of trusted nodes in the network.

Because of mobility nature of MANET, a node can act as a malicious node and degrade the network performance which results in total communication breakdown. In the proposed work, a Secured Network using Promiscuous Mode (SNuMP) is proposed which is a part of Intrusion Detection System. It can repair the malicious nodes in MANET for increasing network performance. Another technique, 2ACKmethod is also proposed for reducing the packet drops. It also concentrates on efficient route discovery process for secure data transfer with packet loss reduction.