

## **Protocols for secure routing and transmission in mobile ad hoc network: a review**

### **ABSTRACT**

Mobile ad hoc network security is a new area for research that it has been faced many difficulties to implement. These difficulties are due to the absence of central authentication server, the dynamically movement of the nodes (mobility), limited capacity of the wireless medium and the various types of vulnerability attacks. All these factor combine to make mobile ad hoc a great challenge to the researcher. Mobile ad hoc has been used in different applications networks range from military operations and emergency disaster relief to community networking and interaction among meeting attendees or students during a lecture. In these and other ad hoc networking applications, security in the routing protocols is necessary to protect against malicious attacks as well as in data transmission. The goal of mobile ad hoc security is to safeguard the nodes' operation and ensure the availability of communication in spite of adversary nodes. The node operations can be divided into two phases. The first phase is to discover the route (s) path. The second phase is to forward the data on the available discovered routes. Both stages need to protect from attacks; so many protocols have been proposed to secure the routing and data forwarding. This is a review study to mobile ad hoc protocols for securing routing as well as protocols for securing packets forwarding. Furthermore, it will present the characteristics and the limitations for each protocol and attributes.

**Keyword:** Securing routing; MANET security; Passive attack; Reactive attack; Security forwarding