**Abstract**

Data security and privacy protection with resource efficiency are the major challenging tasks of wireless Networks. Due to high mobility, untrusted nature is the major challenges faced in mobile networks. Packet dropping and modifications are also common attacks that can be launched by an adversary to disrupt communication in wireless networks. Many schemes have been proposed to mitigate, prevent and tolerate such attacks, but very few can efficiently identify the attackers. Even those schemes could find after the attacks done. Those type of schemes used packet marking techniques to investigate and verify the security issue. The type of implementation is not considered the communication and energy overhead. To address these issues, the proposed system introduces a simple yet effective scheme, which can identify misbehaving forwarders and routes that drop or modify packets. Networks, Encryption; security, Permutation. The proposed system also considers the other type of security issues, in order to identify and prevent the data from unauthorized forwarders, the system proposed a new protocol which is named as **ACT (Anonymous Concealed data Transmission)**. The proposed system utilizes several techniques to protect, prevent and avoid routing misbehaving attacks. In order to identify and block the nodes which tries to drop or modify the data, the proposed system has been implemented the key bit verification algorithm. The procedure behind the proposed system is to identify the key and its value of every packet with concealed data transmission. The proposed system demonstrates that ACT can well protect user data against both inside and outside attackers.