**2.4 Performance analysis of the conﬁdant protocol**

The CONFIDANT protocol works as an extension to a reactive source-routing protocol for mobile adhoc networks. Mobile ad-hoc networking works properly only if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. We propose a protocol, called CONFIDANT, for making misbehaviour unattractive; it is based on selective altruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behaviour of other nodes. The detailed implementation of CONFIDANT in this paper assumes that the network layer is based on the Dynamic Source Routing (DSR) protocol. We present a performance analysis of DSR fortified by CONFIDANT and compare it to regular defenceless DSR. It shows that a network with CONFIDANT and up to 60% of misbehaving nodes behaves almost as well as a benign network, in sharp contrast to a defenceless network.

**2.5 Survey on VANET security challenges and possible cryptographic solutions**

VANET is an emergent technology with promising future as well as great challenges especially in its security. In this paper, VANET security frameworks presented on three parts. The first presents an extensive overview of VANET security characteristics and challenges as well as requirements. The second focuses on a novel classification of the different attacks known in the VANET literature and their related solutions. The third is a comparison between some of these solutions based on well-known security criteria in VANET.In this paper, they have specified certain research challenges and open questions which may be future research directions. Thus enable VANET to efficiently implement a system for trusting vehicles and protect it from any malicious node.