Most recent VANETs routing protocols have neither taken into consideration security aspects nor the available resources at the mobile node. In this research, a security-aware road-side routing protocol with resource estimation methodology (SRSR_RE) for VANETs in a segmented road topology was proposed. The proposed algorithm was modelled by a distributed multi-agent system and to be installed at each road-side base-unit (RSU). The algorithm combines a congestion control unit that adopts a resource estimation mechanism with a secure-route discovery scheme. By such combination, both security and quality-of-service (QoS) requirements are guaranteed, and thus making our VANET robust against security threats besides protecting it from being congested. Compared to the insecure road-side (IRSR) and secure road-side (SRSR) protocols, extensive simulation results show the highest capability of the proposed protocol (SRSR_RE) in maximizing the secure delivery of the data packets and minimizing the end-to-end delays for VANETs with different network’s factors such as nodes density, number of malicious nodes and node’s buffer size.
References


**Index Terms**

Computer Science                            Security

**Keywords**

Keywords Routing, Security, Agents, Distributed Systems, VANETs, QoS, Resource Estimation, ITS, Road Segmentation, Security Threats.