Abstract

The concept of VANETs is quite simple: by incorporating the wireless communication and data sharing capability, vehicles can be turned into a network providing similar services like the ones with which we are used to in our offices or homes. VANETs are distinguished from other kinds of ad hoc networks by their hybrid network architectures, node association characteristics, and new application scenarios. Many traffic signals are used to reduce accidents in the roads, but since it is not much effective. Hence VANET is used; it uses Road Side Unit (RSU). This RSU connects to the internet, and provides information to the Vehicular Ad Hoc Network users. Each and every vehicle is interconnected to each other hence it can send alert message to another vehicle to reduce the speed or increase the speed to avoid accidents. Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such a technology. Every vehicular safety application should be thoroughly tested before it is deployed in a real world to use for. Simulation tool has been preferred over outdoor experiment. In VANET it is requires that a traffic and network simulator should be used together to perform this test. Security scheme, previously proposed in this paper in the presence of attacker definitely improves the performance of VANET. The revise of different security schemes are provides the
suggestion about to propose a new security scheme to secure VANET.

References

Index Terms

Computer Science  Security

Keywords

VANET  RSU  Security  Attack  Ad-hoc