Abstract

Vehicular Ad hoc Networks is a special kind of mobile ad hoc network to provide communication among nearby vehicles and between vehicles and nearby fixed equipments. VANETs are mainly used for improving efficiency and safety of (future) transportation. There are chances of a number of possible attacks in VANET due to open nature of wireless medium. In this paper, we have classified these security attacks and logically organized/represented in a more lucid manner based on the level of effect of a particular security attack on intelligent vehicular traffic. Also, an effective solution is proposed for DOS based attacks which use the redundancy elimination mechanism consists of rate decreasing algorithm and state transition mechanism as its components. This solution basically adds a level of security to its already existing solutions of using various alternative options like channel-switching, frequency-hopping, communication technology switching and multiple-radio transceivers to counter affect the DOS attacks. Proposed scheme enhances the security in VANETs without using any cryptographic scheme.

References

- Yuen Liu, Jun Bi, Ju Yang, "Research on Vehicular Ad hoc Networks,"
Security Attacks with an Effective Solution for DOS Attacks in VANET


- http://www.who.int/en/
- G. Guette, B. Ducourthial, "On the sybil attack detection in VANET", Laboratoire Heudiasyc UMR CNRS 6599, France.

Index Terms

Computer Science

Security

Keywords
Security attack pyramid  Redundancy elimination mechanism