Covert Communication in VANETS using Internet Protocol Header Bit

Abstract

Moving into the VANET (Vehicular adhoc network) makes very beneficial for the vehicles to converse with each other and every node (vehicles) present in the VANET through Intelligent Transport System (ITS). In today’s scenario, Security is a big issue in adhoc networks because adhoc are wireless as like VANETS. VANETS are more prone to attacks due to mobility of the vehicles. Privacy, security and authenticity are some of the required application that is essential before the vehicular adhoc networks are deployed. way. So, to counter such problem, this paper proposes a new scheme that makes use of Covert Channels to secure the data from third party which is also a part of that network.

References


3. Ahmed Al-Haiqi, Mahamod Ismail, and Rosdiadee Nordin, "A New Sensors-Based Covert Channel on Android", Department of Electronic, Electrical and Systems Engineering, National University of Malaysia (UKM), 43600 Bangi, Malaysia, Article ID 969628, 14 pages, Hindawi 2014.


Computer Science, IJES 2009

23. Ankita Agrawal1, Aditi Garg2, NiharikaChaudhiri3,Shivanshu Gupta4,DevesPandey5,TumpaRoy,” Security onVehicularAd Hoc Networks (VANET)”
33. http://www.it.ecei.tohoku.ac.jp

Index Terms

Computer Science  Communications
Keywords

Covert Channel, VANET, ITS, Adhoc, Overt, Subliminal Channel, Steganography.