Abstract

In Vehicular Ad-hoc Networks (VANET), communication can be done with mutual understanding of vehicles. This communication is an important application of Intelligent Transportation Systems. In VANET, safety of user is a main concern, for achieving this vehicles are exchanging safety messages at regular interval to increase the passenger safety on road. But similar to other technology VANET is also suffering from some noticeable issues. From these issues one of the most important issues is security. Since the network is open and accessible from everywhere in the radio range of vehicle nodes, it is expected to be an easy target for malicious users. The availability of the network is extremely needed when a vehicle sends any safety information to other one. In this regard, Denial of Service (DoS) with spoofed IP attacks are very dangerous in VANET because they adversely affect the network availability and very difficult to detect. Oppress the node resources by flooding of messages to the victim vehicle is one of the most dangerous type of DoS attack, in which a malicious node sends a large number of message to the victim node and because attacker uses different ids for doing it, so it is very difficult for a victim to identify that sender of massages is a attacker or a legitimate VANET user.
In this paper, we propose a Neighbor Trust Algorithm (NTA) which is an efficient method to defend against Denial of Service attack (DoS) with Spoofed IDs attacks.

References


Neighbor Trust Algorithm (NTA) to Protect VANET from Denial of Service Attack (DoS)


Index Terms
Computer Science  Wireless

Keywords

Neighbor Trust Algorithm (NTA), Denial of Service (DoS) Attacks, DSRC (Dedicated Short Range Communication).