

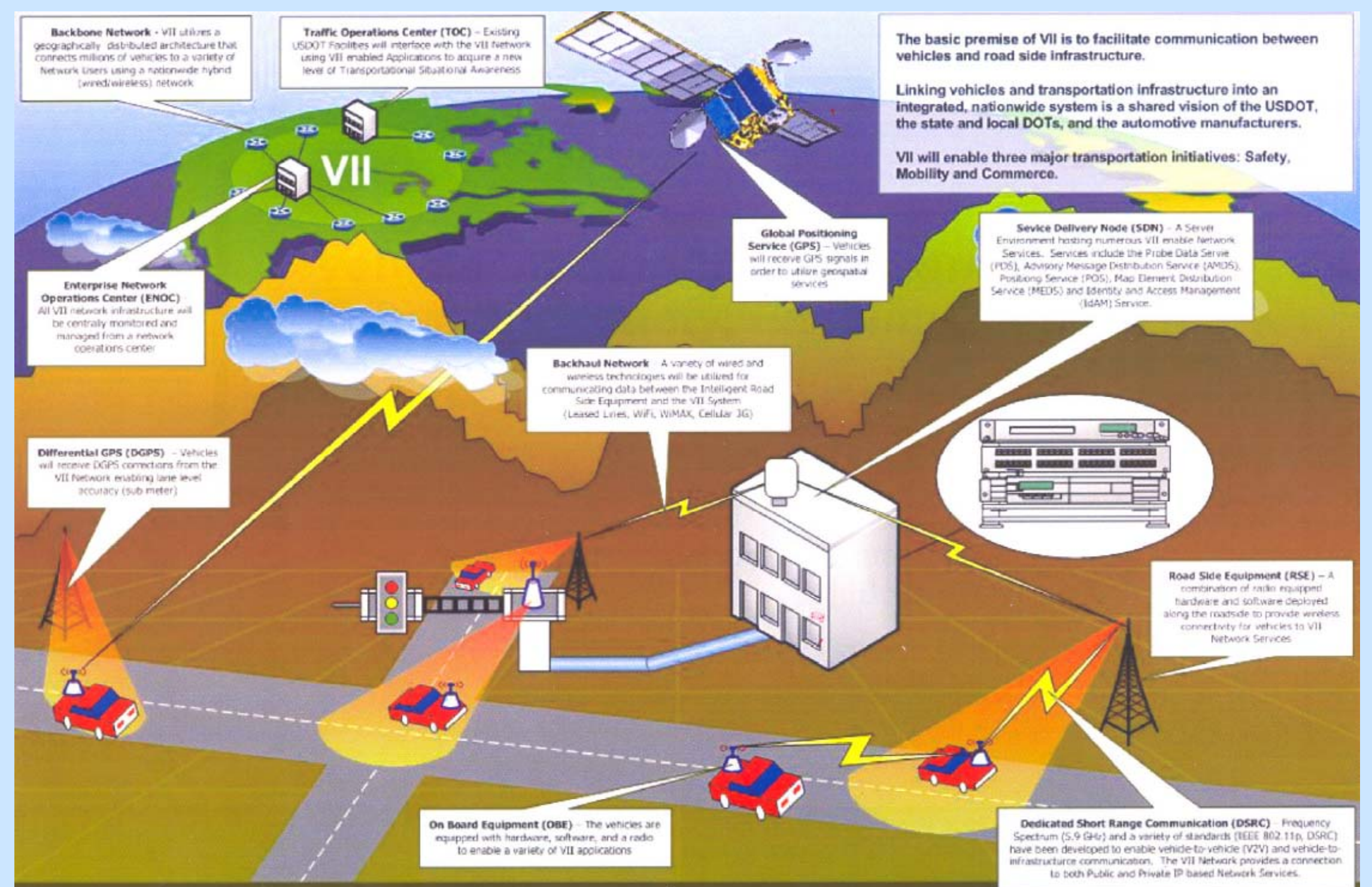


## Trustworthy Transportation Ubiquitous Systems

The potential of Intelligent Transportation Systems and Vehicular Networks in saving lives and facilitating traffic is prompting their rapid development.

Vehicular Networks whereby vehicles and infrastructures are connected through wireless networks exchanging valuable information present two major risks:

1. Vulnerable to attack and abuse
2. Easily overwhelmed



**Vehicular Ad-hoc Network (VANET)**

### Approach and Impact

#### Security in VANET

- Vital signs authentication
- Authentication and key agreement preserving privacy
- Query optimization

#### Research Impact

- Authentication preserving anonymity
- Query optimization algorithms
- Successful technology transfer

We are presently working on an **elliptic curve cryptography-based (ECC)** protocols that preserve vehicle's privacy while ensuring accountability as well as implementing the traditional security services. The proposed protocol has the following advantages:

- It preserves **privacy**;
- It exploits the **difference in capabilities** between resource constrained clients and highly resourceful servers and thus are suitable for wireless applications;
- It **resists known attacks**; and
- It **performs better** in terms of the number of messages and bits exchanged and computing time.