CO515 – Assignment

E/15/202

1. Identify at least three solutions for vehicular communication. (Enabling internet and services on top it for the users moving in the vehicles)

Current solutions for security vulnerabilities in inter-vehicle communication systems.

1) **Certification in VANET (Vehicular Ad-Hoc Networks) Systems**

   In the system called VANET, certification authorities, identification, hardware security module, and secure communication networks are mentioned. Especially in the wireless communication intensive system, the importance of offline protection and data integrity in the vehicle is also given importance.

   Numerous certification authorities are envisaged in the system. These authorities shall be physically separated by zones and each authority shall be responsible for its territory. In order to be used in transit between the authorities, the authorities will certify each other with cross certification and these physical zones will be able to switch vehicles.

2) **Certification in SCMS Systems**

   When the certification methods of SCMS systems are mentioned, a summary can be made as follows. [4]:

   • SCMS manager: works on the definition of misbehavior and the correctness of certificate revocation.

   • Certification services: Describes device types and certification process to be certified.

   • Revoked certificate list repository: maintains and distributes revoked certificates.

   • Revoked certificate list broadcast: Announces the list to all vehicles thanks to road markers.

   Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 June 2017 doi:10.20944/preprints201706.0001.v1

   • Device: Vehicle on the vehicle is the name given to the communication module.

   • Device setup manager: Applies and approves the change of the device's network address or certificate.

   • Certificate registrar: Pseudonym is the authority that approves certifications that describe the pseudonym certificate request permissions of the device during certificate request.

   • Location concealment proxy: When the car makes a connection, the connection is made through a proxy server so that the location of the car is hidden.

   • Misconduct authority: It is authorized to detect misconduct and revoke certificate. It holds a blacklist to be shared with other authorities.

   • Pseudonym Certificate authority: Produces a pseudonym certificate. A particular region or vehicle manufacturer may be limited by features such as vehicle type.

   • Registration authority: evaluates, approves, and transmits Pseudonym certificate requests to the Pseudonym certificate authority.

   • Request editor: Allows a vehicle to not send more than one certificate request in a given period of time

3) **Secure communication in VANETS using Blockchain**

   Blockchain technology can be realized in V2V and V2X communication systems to facilitate the secure distribution of basic safety messages or co-operative awareness messages between vehicles and RSUs and/or the cloud platform. A blockchain framework was proposed focusing on an Intelligent Transport Systems (ITS) infrastructure that contains a wireless module following a Wireless Access in Vehicular Environments (WAVE) or IEEE 802.11p standard. For a secure V2V communication all vehicles broadcast their position through beacon messages (e.g. driving status and position of vehicles), where a location certificate (LC) is generated as digital proof.

2. Explain the implications of using WiFi (IEEE 802.11) for vehicular communication.

Standardization for wireless vehicular communication ensures, as in other domains, interoperability, supports regulations and legislation, and creates larger markets. For the initial deployment of vehicular communication, consistent sets of standards have been created, commonly named C-ITS in Europe and DSRC in the U.S., both relying on the WiFi standard IEEE 802.11. These initial standard sets specify vehicle-to-vehicle and vehicle-to-infrastructure communication and enable applications primarily for driver information and warnings.

Using WiFi in vehicle communications had to face many challenges. Mostly the network security issues. Some challenges faced are,

Routing challenges : - Determining the possible routes in VANETs is hard due to mobility of nodes. The direction, position, and speed of vehicles always change. In this case, even though the source and destination nodes are stable, the location of intermediate nodes changes, which can create packet losses along the path.

Doppler effect:- When two vehicles approach each other due to the Doppler effect, the frequency may be different on the receiver and transmitter side. Therefore, frequency should be regulated on the receiving side.

Hidden terminal problem:- When there is no centralized communication coordination, the hidden terminal problem occurs in VANETs. This causes collisions when two nodes that are not in same communication range try to transmit data to the same node.

Data security:- The privacy of data may be important in some applications. To increase the security, some encoding mechanisms may be used. However, this causes extra overhead on the data and may affect the system performance.

Delay constraints:- In emergency situation, the warning messages have to be forwarded immediately. Due to mobility of nodes and changing in network topology, latency may increase.

And the standard IEEE 802.11 has some performance deficiencies as well.

The most important component of a real-time vehicle-to-vehicle communication system is the MAC protocol method. The MAC of the vehicular communication standard IEEE 802.11 is CSMA, and the researches indicate severe performance degradation for a heavily loaded system, both for individual nodes and for the system.

Location messages will be a central part of vehicle communication systems and much traffic safety application will depend on locations. The researches have indicated how 802.11p should be configured in order to avoid severe performance loss; short packet lengths together with a low frequency range. It should be noted though that if retransmissions are used to increase reliability, the system will be heavily loaded already at low frequencies.

The main drawback with CSMA is its unpredictable behavior. This implies that CSMA is unsuitable for real-time vehicle-to-vehicle communication data traffic. From a sending perspective STDMA outperforms CSMA during high utilization periods. This is much better then CSMA algorithm using the same data traffic model since increased interference can be combined with coding and diversity.

References

https://www.journals.elsevier.com/vehicular-communications
https://www.preprints.org/manuscript/201706.0001/v1
https://www.sciencedirect.com/science/article/pii/S221420961930261X
https://www.researchgate.net/publication/282525798_Standards_for_vehicular_communication-from_IEEE_80211p_to_5G