Abstract

In the thesis, secure and privacy-preserving schemes are designed in vehicular networks, and the specific details of the completed works are shown as following.

Due to the increasing popularity of intelligent vehicles and the recent flourishing of cloud computing, it becomes a recent research trend of extending cloud computing to vehicles by leveraging under-utilized on-board capabilities of vehicles. In vehicular cloud, three security schemes have been designed.

In the first scheme, a novel location privacy-preserving data query scheme is proposed, with the proposed scheme, a data requester can retrieve the data generated by vehicular sensors from the distributive vehicular on-board storage with high accuracy. Since the majority of intelligent vehicles are generally considered as not fully utilized, these vehicles are candidates to provide distributive data collection and storage services. By exploiting the homomorphic Paillier cryptosystem technique and the structured binary scalars to represent the positions of data requesters and the data generating vehicles, the proposed scheme can achieve the location matching of the involved entities with privacy-preservation.

In the second scheme, an efficient data sharing scheme and location privacy-preservation in Internet of vehicles (IoV) is proposed, which enables the collection and distribution of the data captured by vehicular sensors. The data captured by vehicular sensors records a myriad of physical phenomena about the surrounding environments, which enables the data sharing among vehicles and deployed roadside infrastructures to further improve traffic safety and on-board experience in the intelligent transportation system. With the proposed scheme, the multi-dimensional sensory data captured at different locations are first structured by the Chinese Remainder Theorem, then the modified Paillier cryptosystem is exploited to achieve the location privacy-preserving sensory data aggregation. Meanwhile, the proposed scheme exploits the proxy re-encryption technique to achieve the sensory data acquisition at the network edge, without the involvement of the trusted central entity.

In the third scheme, a secure request-response based vehicular data dissemination scheme in the parking lot scenario is proposed. The roadside units (RSUs) deployed in vehicular ad hoc networks (VANETs) can act as information servers to provide information to vehicles under their coverage area. The proposed scheme exploits an invertible matrix to structure multiple data requests, and encrypts the data requests with the homomorphic Paillier Cryptosystem technique. Based on the data requests aggregation, the RSU can recover the individual data request while protecting the unlinkability between the data query and its origin. In addition, the RSU can verify the correctness of the recovered data requests without privacy disclosure by exploiting an identity-based batch verification technique.

To improve the quality of the vehicle-to-infrastructure (V2I) communications, the LTE-A network is brought to vehicular network for its dense deployment, high bandwidth and high-speed movement support. Specifically, two secure handover key establishment schemes are designed.

In the first scheme, a secure handover session key management scheme is designed in mobile relay LTE-A network. To be more specific, a session key is successfully established between the on-board user equipment (UE) and the Donor evolved Node B (DeNB), which is firstly produced by the UE and then securely delivered to the DeNB, which achieves the security goal of the forward and backward key separations. Meanwhile, to decrease the communication and computational burden of the proposed scheme, the proxy re-encryption technique is also employed, i.e., the session keys are initially encrypted by the public key of the mobility management entity (MME) and then re-encrypted by the mobile relay node (MRN), so that the target DeNB can recover the value of the session key with its private key without involving the core entity MME.

In the second scheme, a novel secure coordinated multi-point (CoMP) joint transmission handover key establishment scheme in LTE-A vehicular networks is proposed. Specifically, to achieve the diversity gain brought by the CoMP joint transmission and accommodate to protect the backward/forward key separation, the session key is initially produced by the vehicle and then securely delivered towards the cooperating eNBs, and then decrypted by each cooperating eNB respectively.