Integrating clouds with VANETs

Vimal Kumar and Sanjay Madria (Missouri Institute of Science and Technology)

Bharat Bhargava (Purdue University,   bbshail@purdue.edu)

VANET technology contributes to road safety, dissemination of traffic information, in car infotainment among others. The On Board Unit (OBU) on the vehicle, forms the network and handles the VANET related tasks. OBU however is a resource constrained device, with limited computational and storage capacity. Moreover, VANETs themselves impose high QoS standards on these OBUs owing to their critical nature. Vehicular networks however are critical networks, where disruption of the network, because of malicious or non-malicious intent can lead to loss if integrity and confidentiality. Security in VANETs, which thwarts such malicious intent, therefore is a critical issue. A key component of security is authentication of the vehicles. Before trusting the messages coming from unknown vehicles, the identity of vehicles need authentication. This problem is exacerbated in high vehicle density areas. There are two basic themes; first is the computation heavy schemes such as Boneh et. al's, group signature scheme [2]. The other theme is to store a number of keys on the OBU, which would help authenticate the vehicles, such as the schemes in [1] and [4]. Other schemes such as the one proposed in [3], call for a hierarchical infrastructure setup. Chen et. al's [5] scheme provides low computational and storage overhead but introduces delays. The drawback of all these schemes is that an attacker can easily overwhelm a vehicle's OBU by inundating it authentication messages and keep it in either a computation loop, or result in messages being dropped. Both of these possibilities result in unacceptable delays.

We propose to explore the integration of cloud computing with vehicular networks for providing security solutions. Clouds are becoming an integral part of ubiquitous and pervasive computing paradigm. The integration of cloud computing with vehicular networks has the potential to open up a range of new possibilities. Clouds provide cheap storage and computation power which could be used to relieve the computation and storage overheads of the resource constrained OBUs on the vehicles. The overhead of the storage of huge amounts of data and intensive, time consuming computations can be easily offloaded to clouds. In particular, solutions to challenging security related issues such as authentication of vehicles can be designed using a hierarchy. In this hierarchy the cloud is at the top and the vehicles is at the bottom, with the RSUs in between, creating a roughly tree like topology. Each vehicle has a virtual image in the cloud, which stores metadata about the vehicle, such as the current location, nearby RSUs etc. With this structure in mind, authentication schemes can be redesigned such that the storage and computation heavy work is done on the cloud, with the RSU providing the intermediate infrastructure, while the lightweight authentication of the cloud's response can be done by the OBU. The metadata from the vehicle's virtual images can be used to easily create clusters and perform efficient key management, distribution and revocation in cloud. Since the private/public key pairs and certificates and the computations are offloaded to the cloud, energy expensive but secure cryptographic operations [6] can be easily performed, providing stringent security guarantees, without sacrificing the QoS parameters.

The integration of vehicular networks and cloud computing has opened up a myriad of possibilities. Our approach in this position paper is to provide security and security related tasks for VANETs through clouds by keeping a virtual image for each vehicle in the cloud. Such an approach can be used not just for security but for other VANET services such as infotainment, route calculation and vehicle safety.

References

[1] J.-P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. IEEE Security & Privacy magazine, 2(3):49–55, 2004

[2] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In Proceedings of Advances in Cryptology (CRYPTO), 2004.

[3] B. Chaurasia and S. Verma, Infrastructure based authentication in VANETs, in International Journal of Multimedia & Ubiquitous Engineering . 2011, Vol. 6 Issue 2

[4] M. Raya and J.-P. Hubaux, “Securing Vehicular Ad Hoc Networks,” J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[5] Lyu, Chen, et al. "Efficient, fast and scalable authentication for VANETs."*Wireless Communications and Networking Conference (WCNC), 2013 IEEE*. IEEE, 2013.

[6]Chenxi Zhang, Rongxing Lu, Xiaodong Lin, Pin-Han Ho, Xuemin Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE* , 13-18 April 2008