The System comes from VANET and Cloud

(Secure Token Reward System)

Supriya S. Bichkule[1], Dept. of computer science & engineering ,G.C.O.E, Amravati, India, supriyabichkule@gmail.com

Prof. Pushpanjali Chauragade[2], Dept. of computer science & engineering.,G.C.O.E, Amravati, India.

Abstract— In Vehicular Ad Hoc Networks (VANETs), selfish nodes (vehicles) who do not contribute to the networks are considered as a threat, so vehicles are forced to participate into the network by sharing the information they collect on the road, whereas participation is optional for nodes in vehicular cloud and they are encouraged to participate with incentives as the network utilizes vehicles' underutilized resources to provide services. Hence, it is necessary to have an integrated incentive system for vehicular cloud, which combined VANET and cloud. The incentive system should be able to cover the entire vehicular cloud, including vehicles in the VANET and service providers in the cloud. In addition, the system must be robust against attacks. In this paper, we present an efficient scheme, Secure Token Reward System in Vehicular Clouds. It ensures the scalability of the incentive system and provides mechanism for securing incentive-related messages. Also, issued tokens can be used by vehicles to get services from the cloud.

Index Terms: Vehicular cloud, VANET, Incentive system, Token reward, Security in Vehicular cloud

1. INTRODUCTION

Recently, Olariu et al. [1] proposed the concept of a vehicular cloud, which combines VANET and cloud. A vehicular cloud is a group of largely autonomous vehicles in VANET that contribute their computing, sensing, communication, and physical resources to the cloud. Vehicles' resources and the information exchanged from the vehicles with the cloud can be used in decision making. Vehicular cloud can facilitate in providing services such as parking management, traffic congestion, avoiding accidents, reducing environmental pollution etc. to customers in real time at low cost [2]. By utilizing cloud computing in VANETs, a vehicular cloud could help reduce propagation of redundant data in VANETs and use its resources more efficiently. In current studies on VANETs, multiple vehicles which observe the same phenomena propagate it to other vehicles which can result in redundant propagation of data [3]. This results in vehicles wasting their resources analyzing the redundant data to find relevant information. A vehicular cloud allows vehicles to exchange their collected data with the cloud, where it can be analyzed, verified, organized, stored, and discarded if it is redundant or irrelevant. Cloud then can send needed information to the drivers upon request. Various other applications can also benefit from using a vehicular cloud such as Intelligent Parking Management [4], Intelligent Transportation System using Traffic Monitoring [1],and Planned evacuation system [2].

Vehicles are equipped with computational resources and storage facilities, but they are often underutilized. There are many people and application managers interested in renting such resources as well as obtaining the information collected on the roads. Since the contribution of the vehicles are optional, some drivers may choose not to do it. Drivers can be enticed to contribute the resources of their vehicles by offering incentives. Several incentive schemes have been proposed to entice selfish nodes in MANETs and VANETs, but they are not suitable for vehicular cloud because they were designed only for handling selfish nodes in routing. Hence, there is a need of an integrated incentive system to reward the drivers of the vehicles for sharing their resources as well as to help the people who are interested in resources of the vehicles and information collected by the vehicles on the roads. In this paper, we propose the secure token reward system for vehicular cloud as an incentive scheme to address the issues above. Our scheme is to achieve the following objectives. First, Token transaction should be secure and robust against attacks. Second, Integrity and authenticity of the messages exchanged between entities should be ensured. Third, privacy of vehicles should be protected while contributing their resources for services in cloud and obtaining/using tokens. Fourth, The awarded token can be used for the service in the future.

2. SECURE TOKEN REWARD SYSTEM

In this section, we first introduce the system model and then describe our secure token reward system for vehicular clouds in detail in the rest of the section. Also, the proposed scheme is shown in Figure 1.

2.1 System Model

The secure token reward system proposed in this paper consists of the following entities.

- Service Provider Manager (SPM): The SPM manages all service providers in the cloud and serves as the representative of service providers so it is responsible for advertising services, making contracts for services, validating proofs of works done by vehicles, and issuing tokens as reward to them as incentive for their participation in the cloud.

- Reward Token System (RTS): The RTS serves as the token bank in the cloud. It creates an account for each vehicle when the vehicle is registered and the account is tied to vehicle's pseudo ID. It assigns tokens to the vehicles when they contribute their resources.

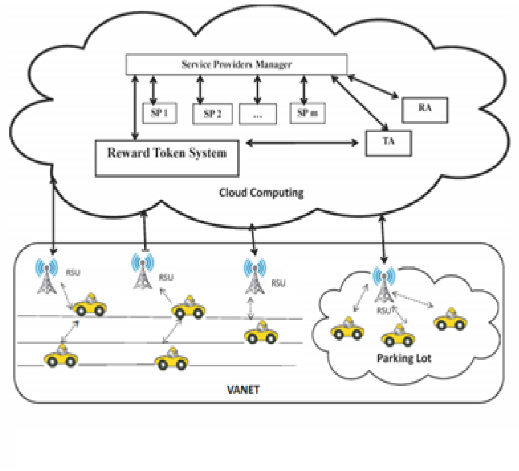

Fig 1: Secure Token Reward System

- Revocation Authority (RA): The RA maintains the revocation list for the misbehaving vehicles. It also Keeps the records of vehicles whose contribution was poor. Once a vehicle is identified as misbehaving vehicle, its certificate is revoked using revocation protocols for the vehicular cloud network.

- Trusted Authority (TA): The TA is in the cloud and is able to communicate with RA, RTS and SPM securely. When a vehicle is registered or renewed, it issues a certificate for the vehicle. And it also manages all private information about vehicles including the certificate, which ties to the vehicle's public key, and (public, private) key pairs. It also helps the SPM in verifying vehicles when needed. The real identity is not given to the SPM, however, when investigations are required by legal authorities, it can reveal the real identity of vehicles to the authorities.

-Road Side Units (RSUs): The RSUs are located along the roads and connected by a network so they serve as gateway to the cloud from the V ANET.

- On Board Units (OBUs): An OBU is a tamper proof device installed on the vehicles. And it has computation, communication capabilities and storage.When a vehicle is registered, its public/private key pair is assigned and the public keys of the RTS and the SPM are stored in the OBU installed in the vehicles. Besides, OBUs on vehicles are able to check the token balance through the RTS.

2.2. Secure Token Reward System

The proposed scheme has the following phases:

Phase 1.Searching Resources: When a cloud service provider looks for vehicles for resources, the cloud service provider manager (SPM) broadcasts a message through the cloud on behalf of the service provider. When an interested vehicle receives the message and decides to contribute its own resource to the cloud for the service, it sends a request message for the work to the SPM in the cloud through the road side units (RSUs). Then, the SPM verifies the vehicle (or driver) with the help of the trusted authority (TA) and checks the previous records stored by the revocation authority (RA) (if there's any). If there are more vehicles interested in contributing their resources than what the service provider needs, the SPM picks vehicles based on their previous record.

Once the vehicle is verified, the SPM signs a contract for the work between the service provider and the vehicle and sends it to the vehicle, so the vehicle can start the work based on the contract. Here, the vehicles use their pseudo ID in all communications to protect their privacy.

Phase 2. Requesting Reward Tokens: After completing the assigned work, a vehicle sends a message with the proof of the work done to the SPM. This proof message helps the SPM in verifying the completion of the work. Note that all cloud service providers are connected to the SPM and the SPM can handle all messages on behalf of the service providers. After the completion of the work is verified, the SPM sends a reward token request to the reward token system (RTS) so it can send tokens to the vehicle as a compensation for the work. When the reward token request is processed by the RTS, a transaction number is generated and sent to the SPM and the vehicle as a confirmation.

Phase 3. Using Tokens for Cloud Service:. In the vehicular cloud, there are various types of services available through cloud service providers. The cloud services generally can be purchased with pay-as-you-go, but the reward token earned by contributing resources into the cloud can also be used as a method of payment for the could services. Since that vehicles are able to check their token balance with the on board units (OBUs), they can simply use the cloud services with tokens if they have enough balance for using the services.

3. CONCLUSION AND FUTURE WORK

In this paper, we presented an incentive based solution called secure token reward system for vehicular cloud to entice vehicular nodes for participating in the network. Our scheme is based on the idea that tokens are given as an incentive to the vehicles who contribute their resources for cloud services. The token reward system located in the cloud ensures the integrity of token transaction and efficient management of tokens. Also, tokens earned for sharing their resources can be used for accessing another services from the vehicular cloud later. In the future, we will work on providing more security features along our secure token reward system and finally apply them towards vehicular cloud architecture.

REFERENCES

[l] S, Olariu, L Khalil, and M, Abuelela, "Taking vanet to the clouds," International Journal of Pervasive Computing and Communications, vol. 7, no, I, pp. 7-21, 2011.

[2] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds," in Ad hoc networks. Springer,2010, pp. 1-16.

[3] K. Lim and D. Manivannan, "An efficient scheme for authenticated and secure message delivery in vehicular ad-hoc networks," in

Proceedings of the 12th IEEE Consumer Communications and Networking Coriference (CCNC), 2015. IEEE, 2015.

[4] S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang, and I. Khalil, "Datacenter at the airport: Reasoning about time-dependent parking lot occupancy," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 11, pp. 2067-2080, 2012.