SIGNATURE SEEKING DRIVE FOR INCENTIVE BASED AD DISSEMINATION IN VEHICULAR NETWORKS

Dr. S. Rajalakshmi¹, S.T. Tharani²

¹Associate Professor, Department of Computer Science and Engineering, Jay Shriram Group of Institutions
²Assistant Professor, Department of Computer Science and Engineering, Jay Shriram Group of Institutions

ABSTRACT

This paper explores the concept of vehicular adhoc network (VANET). Here, the communication nodes are vehicles. Each and every vehicle can communicate with each other and also can communicate with infrastructure for some service. This infrastructure is imagined to be presented along the roads. By using this vehicular adhoc network, the users can have more benefits and services. A promising application over vehicular adhoc network is, an advertiser can use this VANET to distribute their ads through vehicle to vehicle communication. Due to the non-cooperative node (Selfish and malicious nodes), this ad system cannot be realized until the correct incentives and security process are in place. The work describes the Signature Seeking Drive which is the secure framework, which performs the cooperative distribution of ad message between vehicular users in secure manner. The Public Key Infrastructure provided incentive to cooperative nodes. Our proposed work also search to develop an incentive system in which an ad provider can provides the rewards directly to the users and pedestrians also distribute their ads through their smart PDAs.

Keywords - Vehicular Ad hoc Network (VANET), Ad Dissemination, Incentive, Public Key Infrastructure (PKI).

I. INTRODUCTION

This work introduced the vehicular ad hoc network, which performs on the road through the smart vehicle consists of computing resources, sensing devices and short range radios for communicating with other vehicles and also roadside infrastructure. Here, the main thing is networks on the road and it gives some services. An ad distribution through vehicle
to vehicle communication is the most truthful application over the networks. By using this system an ads can be distributed through vehicle to roadside communication by ad provider. Then other vehicles start to distribute those ads by forwarding them to another vehicle while moving when it received the information. Similarly each vehicle can forward those ads continuously for a particular time period. In this, the selfish users don’t want to forward the ads whenever it received the ads. The network by sending out dummy ads, without correct security, that’s why the incentive and security process has been taken.

In such system, Public Key Infrastructure is the best way to satisfy the security requirements in vehicle communication by digital signature. It gives its certified identity and secure location verify scheme. By this authentication, security in VANETs becomes strong. This paper presented one secure incentive framework for ad distribution in VANET which is named as Signature Seeking Drive (SSD). It provides incentive to the users based on their ad services. It just likes a reward which is provided by micropayment charging/rewarding scheme. During the driving, it may collect many receipts. By using this receipt, user can exchange the receipt to virtual cashier and get some cash from receipt-providing nodes. By using this virtual cash, users can fill the gas for their vehicles in gas station.

Goal of the paper

Advertisers in all those types probably want to spread their ads in secure manner. However, from a viewpoint of vehicle users, those commercial ads are only give the benefit to the business companies and they are exploiting vehicle user’s resources for their own profit. Users probably want some type of incentive to stimulate cooperation. Thus the graceful compromise between these two sides is that advertisers pay charges for network resources or advertising charges. Vehicular ad system projected secure incentive framework for commercial ad spread in VANETs which is named as Signature Seeking Drive (SSD). This framework stimulates cooperative distribution of ad messages among vehicular users in a secure way and it also provided the secure ad distribution between the vehicles and pedestrians PDAs.

II. SYSTEM MODEL

In this section to described our vehicular network module.

A.VANET Network module

We used SWANS (Scalable Wireless Ad hoc Network Simulation) vehicular network simulator. SWANS have been shown to be scalable and efficient; it supported the large number of mobile nodes. SWANS fully implemented the IEEE 802.11a protocol. All vehicles in our simulations have a transmission range of 300m. The roadway is a four-lane divided highway of length 100 km. Vehicles are entered into that highway according to the Poisson distribution and travel at a maximum speed of 30 m/s. The simulation is run for 360 seconds and generated the 500 vehicles. In the 360-second simulation runtime, the maximum distance traveled by any vehicle is 10 km. In the high density case there are averages of 90 vehicles / km. In medium density traffic, there is an average of 66 vehicles / km and in low density there is an average of 53 vehicles / km.
In this module we develop a VANET Network model. In that each node (vehicle) can communicate with other nearby nodes (vehicles) to perform some useful applications. Our vehicular network module assumes that, each registered node keeps its own certificate [i.e., public/private key pair issued by a certificate authority (CA)]

**Certificate authority (CA)**

The certificate authority has two roles:
1) Government Authority
2) Vehicle Manufacturer
In this the first one has many administrative problems, the vehicle manufacturer also trustworthy one. So we need to give proper security to our VANET.

**Vehicular Authority (VA)**

The vehicular authority (VA) is the authority provider; it is given the authority to all the vehicles to disseminate their ad in the VANET. The vehicle that get the permission from VANET only disseminate ad in the network. VA also maintain the all ad payment transaction.

---

**Fig.1. Vehicular network module**
B. One Level Advertisement

In one level advertisement the only one vehicle has the authority to disseminate the ad in the VANET. Other vehicles are not having the authority to reuse the ad and this module only suitable for local area communication.

Fig. 2. One level advertisement
C. Multi Level Advertisement

In Multi level advertisement each every vehicles have the authority to disseminate the ad in the VANET. The ad get by the one vehicle, it is nearer to the ad distribution point (ADP). That ad should be reused by all the vehicles that have the vehicular authority over the network. It is suitable for wide area communication.

**Fig. 3 Multilevel Advertisement**
Fig 4. Localized Advertisement
Start

Initial registration of vehicles for VA and CA public key that becomes Advertiser (I) who needs to disseminate their ad request permission from

After approval Advertiser distribute their ad for certain period and certain area

A vehicle (u) agrees to forward I’s ad at Ad Distribution Point (ADP)

Vehicle (u) continues to advertise it to any encountered vehicle or roadside pedestrian’s PDA or smart phone using localization

Receiving vehicle v, returns digitally signed receipt for u. This is called single level ad dissemination

If then v transmits to more nodes/vehicles and digitally signed receipt returned for sender nodes. This is called multilevel ad dissemination

These receipts are exchangeable at VC where VC sends record to VA and it in turn charges advertiser (I)

Stop

Fig. 5. Vanet with PDA
D. Localized Advertisement

In localized advertisement some advisers want to disseminate their ad in particular geographic area, for that purpose we used the localized model. Here we used the Location coordinates (LOCs), S is the ad distributor and RNs is the advertising radius. In this we used two approaches

1) GPS based Approach
2) Infrastructure based Approach

In the GPS based approach to estimated the distance between the two locations, if that value is less than or equal to the RNs, after that only it disseminate the ad otherwise ad is not disseminated in the network. But in GPS based approach we have one disadvantage; in this not verify the receipt providing node authority. It should be satisfied in Infrastructure based approach; in this we verified the receipt providing node authority by using the beacon signal from base station, it should be nearer to the receipt providing node.

E. VANET with PDA

In this implemented the vehicular network with pedestrians Smart PDAs. Whenever the vehicle to vehicle communication (V2V) and vehicle to infrastructure communication (V2I) is not possible that time the advertiser send their ads to the nearby pedestrians Smart PDAs. Through those PDAs, that ad should be disseminating to the nearby vehicle. By using this approach the ad dissemination speed will be increased. In this work also the security overhead may be occurred and it should be managed by our Signature Seeking Drive framework.

III CONCLUSION

The dissemination of commercial advertisements in VANETs is based on practical aspects such as advertising intensity and dissemination locality. With both selfish users (incentives) and malicious users (security) the developed SSD secure incentive framework stimulates cooperative dissemination of ad messages among vehicular users in a secure way. The SSD employs the concept of virtual cash to charge and reward the provision of advertising service as an incentive for users in the network. The performance evaluation results of SSD through analysis and simulation experiments reveal its robustness in both incentive and security perspectives against various types of attacks and it showed the effectiveness of our advertisement models.

REFERENCES