International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015
ISSN 2091-2730

An Effective Strategy for Trusted Information Scheme for Location Privacy in VANETs

Rakesh Kumar ER

Asst. Prof. & Head (CSE),
SAMS College of Engineering and Technology, Chennai
rakeshkumarer@gmail.com,
9842882698

Abstract— VANET can be formed by connecting vehicles with internet access by drivers. Vehicles running with different speed, directions and locations can form ad-hoc network to solve various problems in human life such as traffic management, safety in transportation, utilization of transport resources and many ad-hoc applications for mobile users. Method used for protecting such as clustering, anonymization, fake point location privacy etc. are proposed by different authors. It is important to see that the vehicle's or group of vehicle's location privacy needs to be protected. In this paper we are retracing the technique used for location privacy in VANET and propose the novice Ad-hoc Trusted Information Exchange method for location privacy.

Keywords— VANET, location privacy, ad-hoc trust, mobile security, LOR

INTRODUCTION

Basically VANET is an application of MANET which can be formed by connecting vehicles with internet access by drivers. It plays important role in traffic management and safety driving. In VANET, each vehicle is embedded with OBU (on board unit) and AU (application unit) as shown in fig.1. Where OBU has communication capability and AU is used to execute a program made for OBU's communication capability. Road Side Unit (RSU) can be attached to the infrastructure network which is connected to the internet. VANET provides two types of communication:

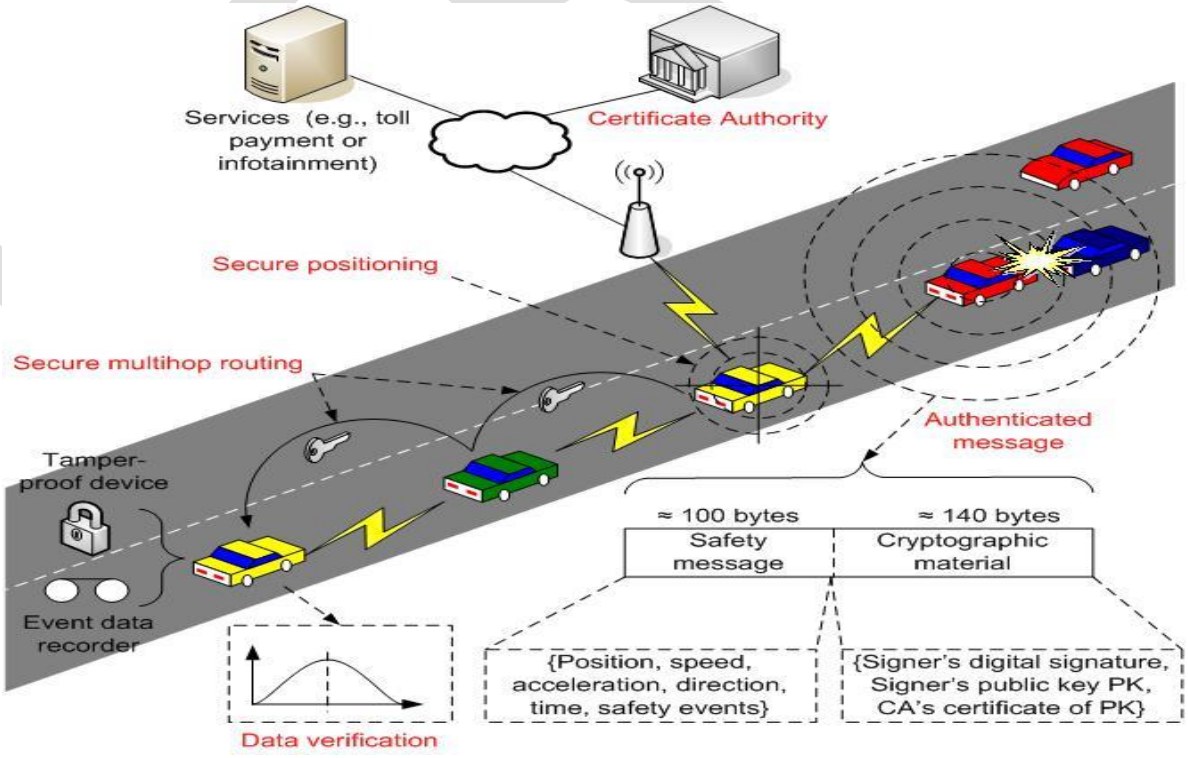

Fig 1: VANET Architecture

1] Pure wireless ad hoc network- vehicle to vehicle. And
2] Communication between fixed infrastructure (i.e. RSU) and vehicle

Location Privacy is nothing but the special type of information privacy which concern the claim of individuals to determine for themselves when, how, and what extent location information about them is communicated to others. Location is inextricably linked to personal safety. Unrestricted access to information about an individual's location could potentially lead to harmful encounters, e.g. physical attacks. Hence location privacy is an important issue in vehicular ad-hoc network.

In this paper we discuss the Trusted Information Exchange Scheme for location privacy in vehicular ad-hoc network. The rest of the paper is structured as follows. Section II describes the related work of VANET's location privacy. Section III describes the threat model and proposed location privacy scheme and section IV presents conclusion.

OVERVIEW OF VANET

Intelligent transportation systems (ITSs) In intelligent transportation systems, each vehicle takes on the role of sender, receiver, and router [4] to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. For communication to occur between vehicles and RoadSide Units (RSUs), vehicles must be equipped with some sort of radio interface or OnBoard Unit (OBU) that enables short-range wireless ad hoc networks to be formed [5]. Vehicles must also be fitted with hardware that permits detailed position information such as Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. Fixed RSUs, which are connected to the backbone network, must be in place to facilitate communication. The number and distribution of roadside units is dependent on the communication protocol is to be used. For example, some protocols require roadside units to be distributed evenly throughout the whole road network, some require roadside units only at intersections, while others require roadside units only at region borders. Though it is safe to assume that infrastructure exists to some extent and vehicles have access to it intermittently, it is unrealistic to require that vehicles always have wireless access to roadside units. Figures 1, 2 and 3 depict the possible communication configurations in intelligent transportation systems. These include inter-vehicle, vehicle-toroadside, and routing-based communications. Inter-vehicle, vehicle-to-roadside, and routing-based communications rely on very accurate and up-to-date information about the surrounding environment, which, in turn, requires the use of accurate positioning systems and smart communication protocols for exchanging information. In a network environment in which the communication medium is shared, highly unreliable, and with limited bandwidth [6], smart communication protocols must guarantee fast and reliable delivery of information to all vehicles in the vicinity. It is worth mentioning that Intra-vehicle communication uses technologies such as IEEE 802.15.1 (Bluetooth), IEEE 802.15.3 (Ultra-wide Band) and IEEE 802.15.4 (Zigbee) that can be used to support wireless communication inside a vehicle but this is outside the scope of this paper and will not be discussed further.

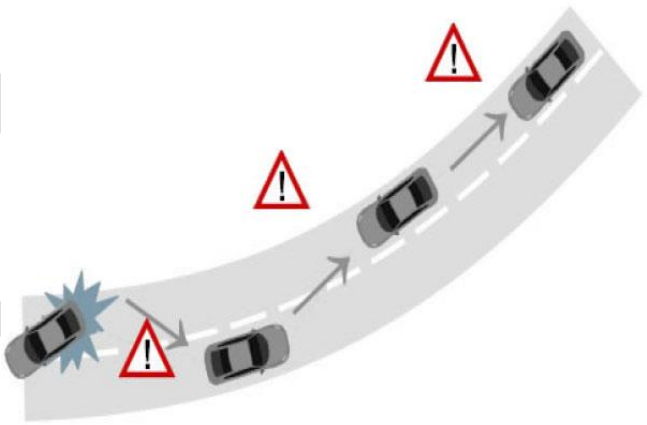

Fig 2: Inter-vehicle communication

A. The inter-vehicle communication configuration (Fig. 2) uses multi-hop multicast/broadcast to transmit traffic related information over multiple hops to a group of receivers. In intelligent transportation systems, vehicles need only be concerned with activity on the road ahead and not behind (an example of this would be for emergency message dissemination about an imminent collision or dynamic route scheduling). There are two types of message forwarding in inter-vehicle communications: naïve broadcasting and

intelligent broadcasting. In naïve broadcasting, vehicles send broadcast messages periodically and at regular intervals. Upon receipt of the message, the vehicle ignores the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it. This ensures that all enabled vehicles moving in the forward direction get all broadcast messages. The limitations of the naïve broadcasting method is that large numbers of broadcast messages are generated, therefore, increasing the risk of message collision resulting in lower message delivery rates and increased delivery times. *Intelligent broadcasting* with implicit acknowledgement addresses the problems inherent in naïve broadcasting by limiting the number of messages broadcast for a given emergency event. If the event-detecting vehicle receives the same message from behind, it assumes that at least one vehicle in the back has received it and ceases broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the vehicles. If a vehicle receives a message from more than one source it will act on the first message only.

B. The vehicle-to-roadside communication configuration (Fig. 2) represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the vicinity. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. The roadside units may be placed every kilometer or less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside unit will determine the appropriate speed limit according to its internal timetable and traffic conditions. The roadside unit will periodically broadcast a message containing the speed limit and will compare any geographic or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the vicinity. If a vehicle violates the desired speed limit, a broadcast will be delivered to the vehicle in the form of an auditory or visual warning, requesting that the driver reduce his speed.

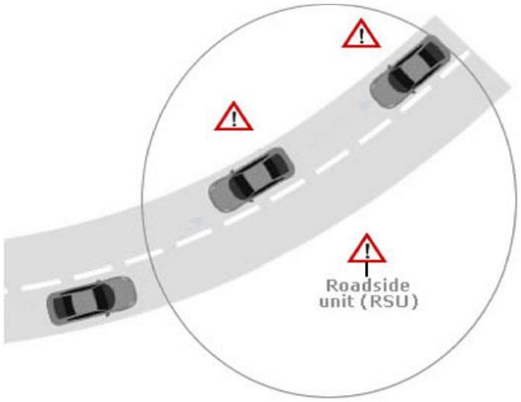

Fig 3: Vehicle-to-roadside communication

C. The routing-based communication configuration (Fig. 3) is a multi-hop unicast where a message is propagated in a multi- hop fashion until the vehicle carrying the desired data is reached. When the query is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source.

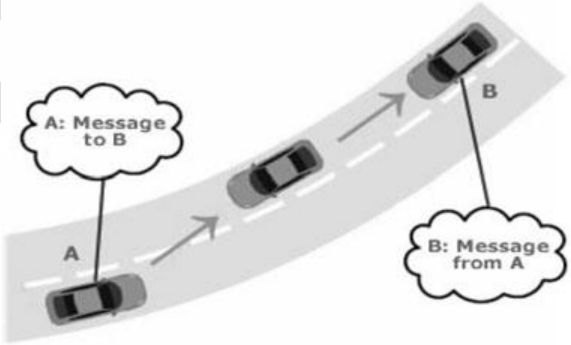

Fig 4: Routing-based communication

LITERATURE SURVEY

There are many solutions provided to achieve location privacy in VANET. We have taken some of them and following are their descriptions:

A. Endpoint Protection Zone (EPZ)

In [1] George Coser et al proposed location based services (LBSs) and designed it in such a way that all the LBS users are clustered by spatial location into endpoint protection zone. Login credentials are shared by all the users from the same EPZ and users remain transmission silent in their EPZ. That means they won't send any query to LBS or send safety message to other vehicles until they left their own EPZ. As no any information is sent through that region adversary or LBS admin cannot identify the user's location. If the LBS admin can correlate source and destination's coordinates, they can easily find the real identity and location of vehicle. This is not possible if a vehicle remains transmission silent in their respected EPZs. Disadvantage of this model is, it is not effective in sparsely dense areas.

B. Fake Point Location Privacy Scheme

[2] Presents the idea of concealment and power variability named Fake Point for the purpose of location privacy. The main concept is to choose a location among the available hotspot. These fake points are considered by mobile devices (MNN) while calculating their transmission signal power. Hence, if one of the attacker's mobile devices is placed at the fake point, then its Received Signal Strength will be same for those mobile devices who selected that FP. In such a way error in mobile network nodes distances, estimated at this FP, increases and made deviations in the adversary's estimation of location and hence the MNN's location privacy is ensured.

C. Clustering Anonymization

In [3] Bidi Ying et al proposed a method called Protecting Location Privacy with Clustering Anonymizatiom (PLPCA) for location based services in vehicular ad hoc network. This PLPCA algorithm converts road network to edge-cluster graph for hiding traffic and road information. It will also offer the clocking algorithm to conceal a target vehicle's location. Clocking algorithm is based on k-anonymity and l-diversity. As per simulation analysis PLPCA has good performance in hiding the road information.

D. Efficient Pseudonym Changing Schemes

In [6] Pseudonym changing schemes considers three factors i.e. age of pseudonym, speed and moving direction of vehicles. Based on these parameters Yeong-Sheng Chen et al developed four mechanisms AD, AD, SD, ADS. Age of pseudonym means the time interval for which pseudonym is used. Vehicle will try to change its pseudonym over a specific time interval. Longer the pseudonym name, less the location privacy. Pseudonym change should be performing while changing the direction of vehicle. All the above mechanisms have better performance.

E. Privacy by Decoy

George Corser et al presents a privacy protocol [9] named PARROT i.e. Position Altered Requests Relayed over Time and Space. It protects the information about location of LBS users. In this method, helper vehicles are called as parrots and the vehicle who wants privacy is known as pirate. Parrot transmits the request to LBS on the behalf of pirate using pirate's login credentials and their own location. In short, parrot sends encrypted message of pirate along with the parrot's location. Therefore, LBS admin cannot identify which location is the location of pirate. The disadvantage of above method is, network congestion overhead increases because of multiple duplicate transmissions of parrots.

F. Pseudonym Changing at Social Spot (KSDP model)

Rongxing Lu et al introduce Pseudonym changing at social spot [4]. Social spots are nothing but the areas where vehicles gather together, for example parking at shopping malls or road intersection when traffic light becomes red. They present the KSDP model in which OBU device in the vehicle has number of anonymous short time keys. These keys are authorized by trusted authority (TA). Keys have not been directly preloaded in the vehicle by TA; instead of that TA provides keys to user- owner of the vehicle. User keeps these keys at home. Whenever user wants to go outside the home for traveling e.g. for fueling, he will supposed to install keys in his vehicle's OBU device. After that when vehicle runs in urban area, these short term keys can be used for transmitting the messages. As authorized keys are not installed in vehicle itself, vehicle thieves cannot generate short term keys and thus mitigate the vehicle theft.

PROPOSED WORK

In this section, we are describing and formalizing different techniques to demonstrate how privacy threat can occurs and our ad-hoc trusted exchange protocol for location privacy. In this paper firstly we are going to design the inference modules as shown in fig.2, and then we will propose the protocol for privacy against these inference modules.

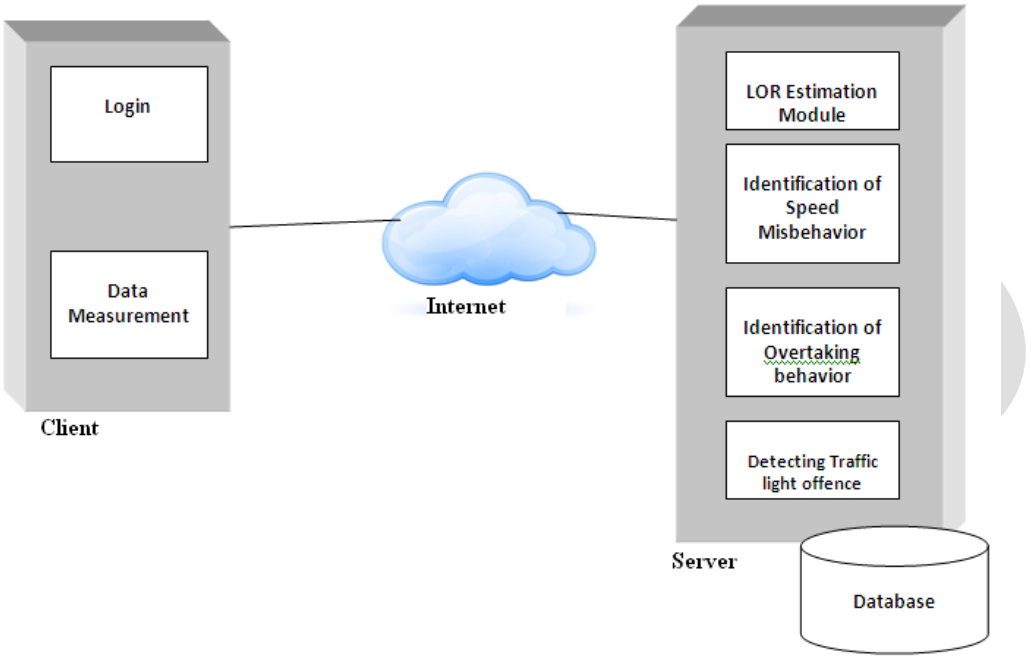

Fig 5: Threat model in our scheme

Whenever LBS user (client) sends request to LBS administrator (which might be the attacker), LBS admin can find the LOR (locality of reference) based on the number of request send by the particular user within a specific time of interval. Attacker also can find the speed of vehicle using monitoring devices and using this information he can try to attempt the attack on vehicle.

A. LOR Based Threat

This module is for estimating the locality of reference. We can find the locality of reference based on number of requests sent by LBS user. We first divide the total time of monitoring T into some time intervals, say where i=1,2,….n. Within the t1 time interval which location is frequently asked by user is calculated and the sampling rate of this can be estimated. Here Sampling rate is nothing but the frequency of changing the location request by the user. If sampling rate will be more than threshold value, user's location is difficult to find whereas if sampling rate will be less i.e. if user requests for the same location multiple times, it will be easy to find his location. LOR based threat is shown in fig. 6.

B. Speed Misbehavior Threat

Once we get coordinates of user sending query and his time to reach the desire location, we can get the speed of that user. As VANET is self organized network, we assume all vehicles should travel cooperatively by setting up same speed. If vehicle appears moving with dissimilar speed, it means it might be an adversary. We can examine the variations in vehicle's speed to uncover the adversary.

C. Threat by Overtaking Behavior

Overtaking behavior of vehicle can be computed by continuous verification of changing coordinates of vehicle. If the vehicle's coordinates move towards left it will be ok but if they moves towards right, it indicates the overtaking misbehavior of vehicle.

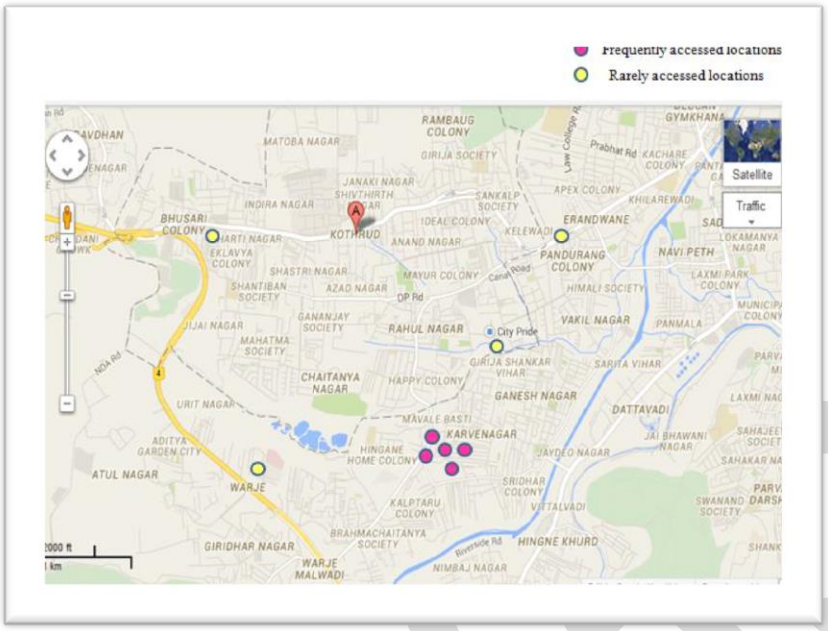

Fig 6: LOR based threat

D. Ad-hoc Trusted Information Exchange

This system consists of ITS (Identity & trust server) and TAS (Trusted Authority Server). ITS is used for verification of vehicle's and user's identity and trust level. As we discussed we can achieve location privacy of the person or the node or the system using this algorithms in VANET.VANET has very huge application area and so the threat to the system. Let us discuss the scenario. This VANET can be used by the daily commuter to get private car providing as well as professional cab service (TSP i.e. Transport service provider). Although there is no need of sharing exact location. The devices in the close proximity will have the share of the information. The request for the commute will be routed through identity and trust verification server to the cars or whatever needed vehicle in nearby vicinity. The identity of both parties will be introduced to one another only when those are in 100 meters of close proximity. All the devices get authenticated by the identity and trust verification. Services are the trusted services who has verified and reliable database of the all users so as to verify users and give trustworthy communication in between the two parties.

CONCLUSION

VANET is an application of MANET which can be formed by connecting vehicles with internet access by drivers. It plays important role in traffic management and safety driving. Location Privacy is nothing but the special type of information privacy which concern the claim of individuals to determine for themselves when, how, and what extent location information about them is communicated to others. VANET has very huge application area and so the threat to the system. As we have discussed we can achieve the location privacy of the person or node using the above method in VANET. As in proposed method a person won't share the location with the service provider hence achieve the location privacy.

REFERENCES

[1] George Corser, Huirong Fu, Tao Shu," *Endpoint Protection Zone (EPZ): Protecting LBS User Location Privacy Against Deanonymization and Collusion in Vehicular Networks*", 2013 International Conference on Connected Vehicles and Expo (ICCVE).

[2] Sanaa Taha, Xuemin Shen," *Fake Point Location Privacy Scheme for Mobile Public Hotspots in NEMO based VANET*", IEEE ICC 2013 - Communication and Information Systems Security Symposium

[3] Bidi Ying et al ,"*Protecting Location Privacy with Clustering Anonymization in Vehicular Networks*", 2014 IEEE INFOCOM Workshop on Dynamic Social Networks.

[4] Rongxing Lu et al,"*Pseudonym Changing at Social Spots: an effective Strategy for Location Privacy in VANETs*",IEEE transaction on vehicular technologgy,VOL.61,NO.1,January 2012.

[5] Ram Shringar Raw et al," *security challenges, issues and their solutions for vanet*", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.

[6] Yeong-Sheng Chen et al," *Efficient Pseudonym Changing Schemes for Location Privacy Protection in VANETs*", International Conference on Connected Vehicles and Expo (ICCVE),2013.

[7] X. Liu, H. Zhao, M. Pan, H. Yue et al, "*Traffic-aware multiple mix zone placement for protecting location privacy*,"INFOCOM, 2012 Proceedings IEEE, pp. 972–980, Mar. 2012.

[8] Xiaomin Ma et al," *Design and Analysis of a Robust Broadcast Scheme for VANET Safety-Related Services*", ieee transactions on vehicular technology, vol. 61, no. 1, january 2012.

[9] George Corser et al, "*Privacy-by-Decoy: Protecting Location Privacy Against Collusion and Deanonymization in Vehicular Location Based Services*", 2014 IEEE Intelligent Vehicles Symposium (IV) June 8-11, 2014

[10] Shokri, R., Freudiger, J., & Hubaux, J. P. (2010*)." A unified framework for location privacy. 3rd Hot Topics in Privacy Enhancing Technologies (HotPETs).*"

[11] Ying Mei et al, "*A Collaboratively Hidden Location Privacy Scheme for VANETs*",International journal of Distributed Sensor Networks Volume 2014, Article ID 473151