Security Experiments in Mobile Devices and its Ad-hoc Networks

Smita K. Suryawanshi
Research Scholar
Department of Information Technology
MIT College of Engineering Pune, India
Suryawanshi.smita1@gmail.com

Balaso N. Jagdale
Associate Professor
Department of Information Technology
MIT College of Engineering Pune, India
balasaheb.jagdale@mitcoe.edu.in

Abstract **– VANET can be formed by connecting vehicles with internet access by drivers in order to improve driving safety. 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. Different authors proposed Location protecting methods such as clustering, anonymization, Privacy by decoy, fake point location privacy etc. It is important to see that the vehicle's or group of vehicle's location privacy needs to be protected. In this paper, aim is reviewing the technique used for location privacy in VANET and proposes the novice Ad-hoc Trusted Information Exchange method for location privacy.**

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

I. INTRODUCTION

The formation of VANET is depends on the connected vehicles with internet access by drivers. It plays vital role in traffic management and safe driving. It is one of the most important applications of MANET.

As shown in fig.1, each vehicle is implanted with OBU (on board unit) and AU (application unit). 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. There are two types of communication in VANET:

1] Pure wireless ad hoc network- vehicle to vehicle. And

2] Communication between fixed infrastructure (i.e. RSU) and vehicle

When data is compromised the whole system suffers. The nature of VANET like predictable movements of nodes or high mobility of victim/attacker could lead to malicious attacks. Adversary could break the system by using attacks such as black hole attack, feed false information etc. Therefore security measures must be taken to avoid the malicious attacks on the system.

Location Privacy is special type of information privacy according to which the individual can determine for himself when, how, and what extent location information about him 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 key issue in vehicular ad-hoc network.

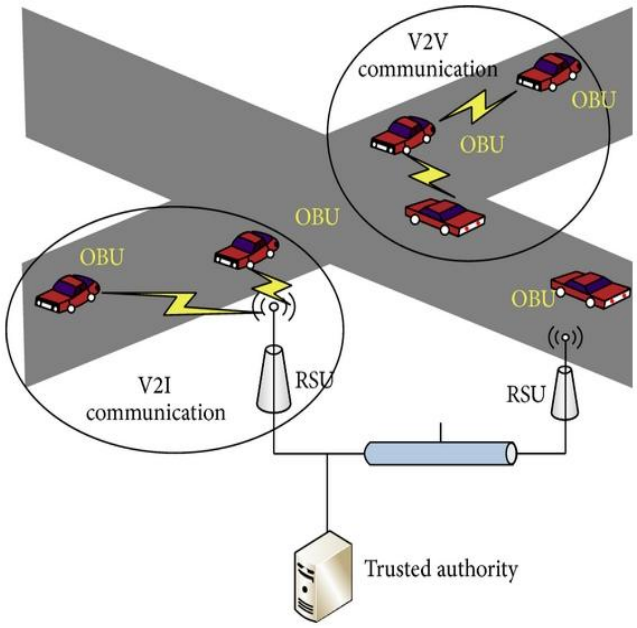

Fig. 1 VANET Architecture [11]

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

.

II. 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: 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 chose 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.

Advantage: 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.

Disadvantage: 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.

III. PROPOSED WORK

In this section, we are describing and formalizing demonstration of different inference techniques and our ad-hoc trusted exchange protocol for location privacy.

Architecture Under Study

In this paper initially 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.

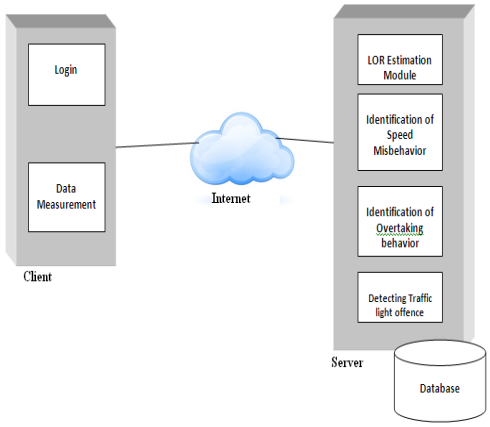

Fig. 2 Threat model in our scheme

A. LOR Based Threat

This module estimates the locality of reference. We can find the locality of reference based on number of requests sent by LBS user. First of all divide the total time of monitoring T into some time intervals, say where i=1,2,….n. Within first time interval which location is asked by user is calculated, the same can be calculated for rest time intervals. At the end calculate sampling rate for all the time intervals.

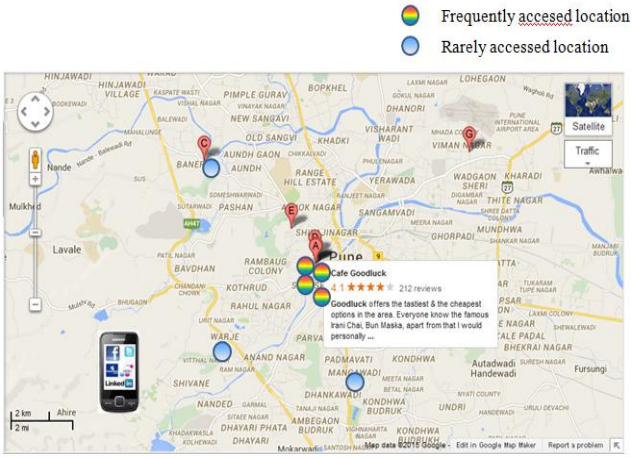

Fig. 3 LOR based threat

Here Sampling rate is the frequency of change of 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 is easy to find his location. LOR based threat is shown in fig. 3.

B. Speed Misbehavior Threat

Once we get coordinates of user sending query and his time to reach the desire location, speed of the user can be determine. We can check the variations in vehicle's speed to expose the adversary. Let be average speed of vehicle and be the threshold speed value

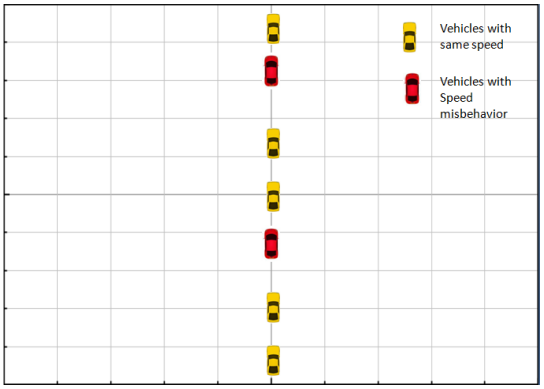

Fig. 4 Speed misbehavior threat

Algorithm: Speed Misbehavior Check

1: Procedure Speed Misbehavior Check
2: Set Threshold Value
3: Calculate average speed of vehicle
4: if > then indicate as misbehaving vehicle
5: if then no misbehavior
6: End procedure

C. Threat by Overtaking Behavior

Overtaking behavior of vehicle can be computed by continuous verification of changing coordinates of vehicle. As indicated in fig. 5, 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.

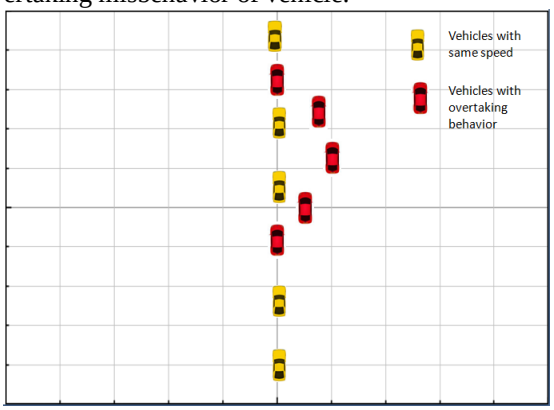

Fig .5 Overtaking behavior of vehicles

Algorithm: Overtaking Behavior Check

1: Procedure overtaking Behavior Check
2: Get the (x, y) coordinates of vehicle
3: Set threshold value for (x, y) coordinate
4: if x > && y > then indicates overtaking behavior of vehicle.
5: else no overtaking behavior.
6: End procedure.

E. Ad-hoc Trusted Information Exchange

This system consists of ITS (Identity & trust server) and TAS (Trusted Authority Server) as shown in fig.6. ITS is used for verification of vehicle's and user's identity and trust level. As discussed location privacy of the person, the node or the system can be achieved using the algorithms in VANET. VANET has very enormous application area and hence the threat factor caused to the system increases. The scenario for the same is mentioned below. VANET can be used by 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 share 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.

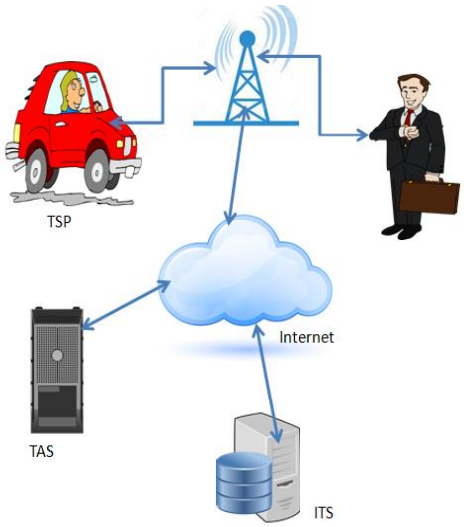

Fig. 6 Ad-hoc Trusted Information Exchange Protocol

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.

IV. CONCLUSION

There are many applications of MANET. Out of which VANET is widely used which is formed by connecting vehicles using internet access by drivers. It plays an important function for traffic management and safe driving. Location Privacy is special type of information privacy according to which the individual can determine for himself when, how, and what extent location information about him is communicated to others. We can achieve the location privacy of the person using the above technique in VANET. In our proposed scheme a person does not share the location with the service provider hence achieves 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.