International Journal of Engineering Research & Management Technology

May- 2015 Volume 2, Issue-3
ISSN: 2348-4039

Email: editor@ijermt.org www.ijermt.org

"Sharpening Skills..... Serving Nation"

Special Issue: 2nd International Conference on Advanced Developments in Engineering and Technology
Held at Lord Krishna College of Engineering Ghaziabad, India

Caravan: A Solution for Vehicle Privacy in Vehicular AD-HOC Network

Atul Singh, Lalit Chauhan, Rishabh Chauhan
B.Tech Student
Department of CSE
Lord Krishna College Of Engineering
Ghaziabad

Saurabh Kumar Gaur
Assistant Professor
Department of CSE
Lord Krishna College Of Engineering
Ghaziabad

ABSTRACT -
In vehicular ad hoc networks (VANET), it is possible to locate and track a vehicle based on its transmission during communication with other vehicle on the roadside infrastructure. In past year mobility and seamless handoff management is one of the challenging issues in vehicular Ad-hoc Network. The traditional Handoff method cannot meet the requirements of the VANET due to high mobility intermittent connectivity and unreliable wireless connection environment.
In VANET the challenging issue is to provide the privacy of the vehicle (User) in this type of the wireless networks. In this paper we study the problem of providing location Privacy in VANET by allowing vehicle to prevent tracking of their broadcast communication, location and other confidential information. We must first identify the unique characteristic of VANET that must be considered when designing suitable location privacy solution.
We proposed a Location privacy schema Called CARVAN which provide location privacy in V2I (Vehicular to Infrastructure) and V2V (vehicle to Vehicle) infrastructure. In this System model, the first aspect that we use the silent period to provide unlinkability between locations.
The second aspect is that use of group concept to avoid overhearing pseudonyms.
The third aspect that is, leveraging group to provide unlinkability between pseudonyms and LBS application.
The four aspects is that, discussion of attacks and solution for proposed scheme.

INTRODUCTION

In this paper we study about the VANET system (vehicular ad-hoc network).Vehicle connected to each other's through an ad-hoc formation form a wireless network called "VANET" (vehicular ad-hoc network) .Vehicular ad-hoc network are a sub group of mobile ad-hoc network (MANET) VANET (Vehicular ad-hoc network) is defined in two types -V2V (vehicle to vehicle) and V2I (Vehicle to infrastructure) communication VANET will become world's largest ad-hoc network. Vehicle is important component of ITS(intelligence transportation system).and in this system ad-hoc means to a system of network element that combine to form a network requiring little or no planning. in this paper our main purpose is to provide privacy for VANET and here we use the Pseudonym for hide the VANET identity and where Pseudonym is a taken word from Greek word where Pseudonym means "false name" with the help of Pseudonym we can hide the vehicle identity from other vehicle so no any other vehicle can achieve the other vehicle identity. In VANET system our main purpose we use two type of communication.V2V (vehicle to vehicle) and V2I(vehicle to infrastructure).Roadside infrastructure (communication) such network present various functionalities in condition of vehicular, security , safety and

location based service(LBS) application. In this paper the problem of any vehicle to be able to found without connection between two or more of its locations in the presence of tracking by an adversaries. Some of points in VANET for privacy

1: we use the silent period time to provide unlinkability between two or more locations.

2: our second point is to identify the group navigation of vehicles can be used for providing location privacy in vehicular ad-hoc network.

3: we leverage the group to provide "GUMNAM" excess to location based application and show. When such a solution can preserve vehicle user privacy.

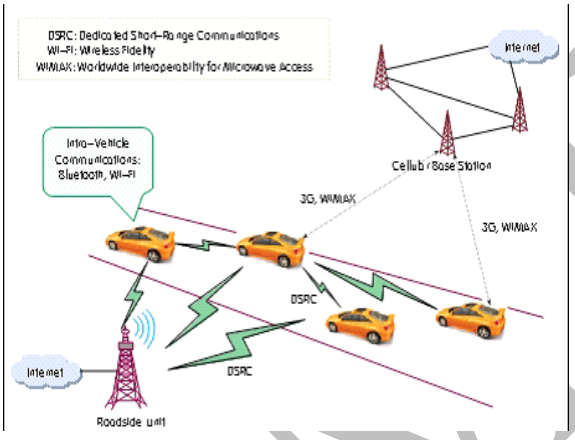

Fig. 1 Inter vehicle communication system and Components

System model

1) Presume and system model of VANET

Fig1: elaborate veritable VANET that comprise of vehicles, retrieve points on road side, and aggregation of location servers. On road vehicles moves and sharing corporate environmental data between themselves and with the servers via retrieve points.

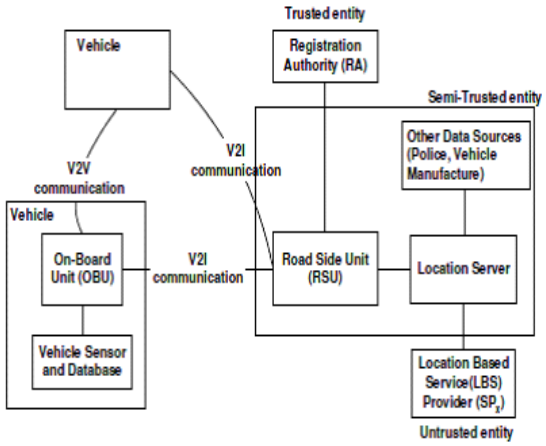

Fig 2-inter -vehicle communication system

Fig2: elaborate a elucidate view of our system model. A vehicle is altering with on board connexion unit for V2V and V2I connexion and sensor and database unit to roll up surrounding data. The connexion unit of retrieve points is known as Road Side Unit (RSU) which is link up to location server locating information is recorded by location server which is forwarded by RSUs and cognition the data together with data from other sources. Location servers also supply an intersection for location based service provider. A confined, RA supply validation and authority service to both vehicles and LBS providers.

1) Confide presume and antagonist model

The admitted base in RSUs and locating server are semi-confined to control as expected. To boot imagine, RSUs are competent to estimation location of vehicle settled based on vehicles transmit signal. In model, we adopt a global passive antagonist. Such antagonist competent to over hear all the broadcast of all vehicles and judge their location.

2) Petition premiss considered

VANET petition have three typical classes

1) Location based services(LBS)
2) Cooperate driving
3) Probe vehicle data

Mobile network is proposition by the LBS petition. To attain most recent celestial point in order to supply request asking service, LBS petition is used. For example : the service may question by vehicle to check out nearby bus stop to steam location In cooperate driving petition, very short distance is maintained by adequacy equipped vehicle between themselves and move suave with same convey speed. The connexion is possible between vehicles may be directly or via connexion equipment provided on road side. In proto type, cooperate driving broadcast their status data i.e., speed acceleration location etc in every 500ms. This petition is to increase safety.

The probe vehicle information represents a class of V2V communication based petition that monitor traffic and road conditions by assembling information from vehicles that are equipped with short range radio or existing long range deed devices. Vehicle recognition, route portion identity, link time and location may be include in probe data and functional status of the probe vehicle equipment, and any other data can be measured and transmit by the vehicles. The RSUs sends probe data requests over a seizure range and vehicles in the seizure range and vehicles in the seizure range reply to the requests. The period between broadcasts of probe replies from vehicles depends on the requirement of covering.

D) Pertinent Constraints of VANET

VANET constabulary constraints such as in mobility of vehicle and in safety petition requirements. The unique characteristic of mobility of vehicle can be observed by:

(1) The movement of vehicles is spatially confined.

(2) The vehicles are spatially qualified on each other in movement.

PRIVACY FOR VANET

Privacy allows for a vehicle to communicate with other vehicles without open its permanent identity. According to Beard, the world Pseudonym is derived from the Greek words and Pseudonym is combination of two Greek words "Pseud + onyma "where Pseud means "false" and onyma means "name" this concept is used for vehicle privacy with the help of Pseudonyms, we hide the original or true identity In forms of VANET using a false name for a vehicle means that vehicle message originated from cannot be traced. The main purpose of "false

name "is so that the vehicles identity should be different for each communication and it would be possible to determine what identity be the same vehicle will have at a later time.

The present caravan the proposal location privacy scheme for VANET and describe the increase technique that constitutes Caravan. Some points are given in Caravan

In order to find a connection between two locations a vehicle can simply update proposed location privacy scheme for VANET. Our main purpose in this topic to provide privacy

Following some points who that provide privacy

A) Use of silent period to provide without connection between locations. When we update the pseudonyms (means false name) then it is hush applicant to join the new and old false name of the node using temporal and spatial relative between new and old position of the node and In this paper, we use a random silent period between update of false name and so in this paper we used the silent period to provide without connection to vehicle entering the network by enforcing that the vehicle will remain silent for a randomly select silent period.

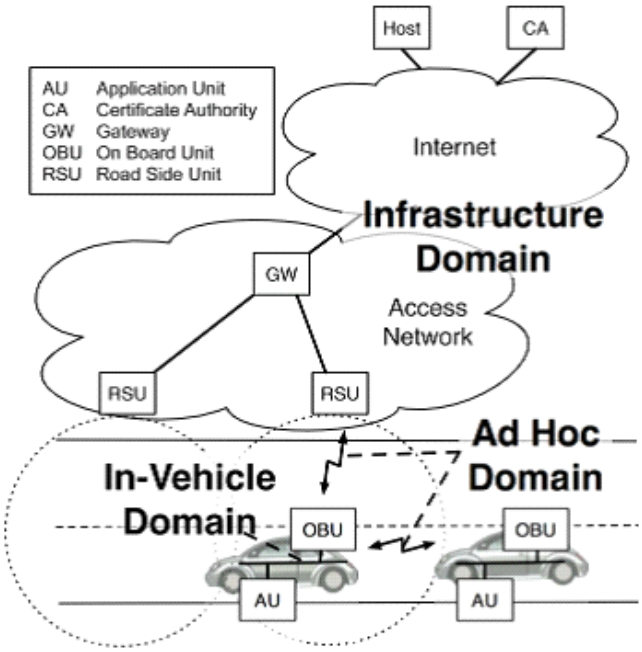

Figure 3 - VANET System Architecture

B) Our second aspect is, use of group concept to avoid over heading pseudonyms

In order to form group concept we restrict the vehicles to be in a group if each group candidate can hear Broadcast of every other group candidate. So each vehicle in a group will move relative to each other and on average have the same velocity. A group can be represented by single vehicle but we refer to as group leader

-> Vehicle in geographical proximity often share redundant information such as road and traffic condition. Hence in vehicle base application such as probe vehicle data.

C) Leveraging group to provide unlinkability between false name and location based application

For successfully link a vehicle pseudonym with real identity of vehicle. When user access an Location based server (LBS) application in an known area it becomes possible to identify the (LBS) application can make use of group leader as proxy for anonymous access. We describe this access protocol below:

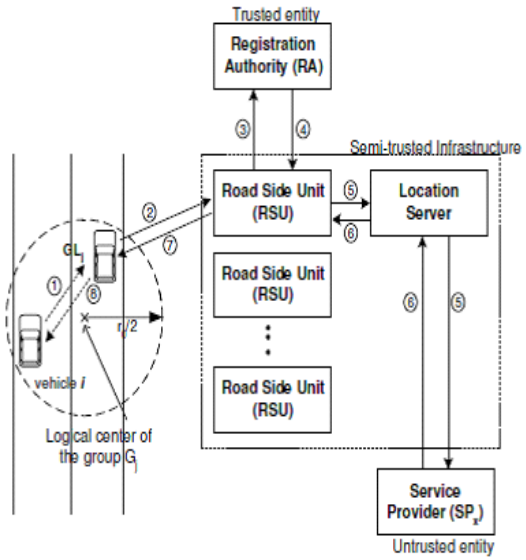

Fig-4 the anonymous access to LBS application

1) Protocol description: application request receiving from vehicle ungroup leader GLj of i's group Gj forward request with its self address to registration authority via the (RSU). The application request validate by RA, then provides session key Kx, i too both service provider (SPx) and vehicle i

2) Group key and application address range:

In this topic, in generate the user request vehicle I perform the two points

1) Suddenly select an available address Aaa from a known user address range of the group Gj
2) Broadcast the user request and encoding with the group of KGj and with Aaa as a source address

These two steps are describing the group Key and application address range and the group key and the address range are obtained by the group candidate Gj from GLj.

D) Hash out of attacks & solution for proposed scheme representation.

1) Intromission false data:-

Misdeed & broadcast incorrect data via media of VANET with indicative intent of attacking by its nearby vehicles. Safety message broadcast the identity of misdeed vehicle verifiably determined to prevent attack on vehicle.

3) Local active offender

The group leaders conspire with the opponent then the obscurity of the vehicle we accessing the LBS application can be separate under the global opponent model. In order to link vehicle I to the LBS application. We propose too defense mechanism against attack by a compromised group leader

1) We propose the use of verification of mixing to cross-check that operation is used by the group leader the LBS application request.
2) A second defiance mechanism is the group leader rotation protocol that limits the attack by the compromised GLj to only a certain rotation period

3) Theatrical attack

A random 'Nickname' can't be proposed by vehicle it must be include registration authority (RA) which is certificated in safety messages .A vehicle i impersonate another vehicle by its overhead nickname. However,

each and every vehicle broadcast safety messages to theatrical role i to its corresponding private key. Therefore theatrical /terrorist attack can be avoided in VANET.

CONCLUSION

VANETs are able to offer safe roads and spacious driving. Some of their diligence has been hash out and it is easily seen that VANETs have much possible. There are however trouble that may originate should the VANET not be protected. As can be seen from the evidence given above, without seclusion, plain hallmark is not enough to maintain a assure system. Hallmark alone permit for tracking and secrecy alone does not provide for trust as the user is not veritable. Therefore, both hallmark and secrecy are necessary in a VANET.

REFERENCES

1. Z. Li, Z. Wang, and C. Chigan, "Security of Vehicular Ad Hoc Networks in Intelligent Transportation Systems," in Wireless Technologies for Intelligent Transportation Systems, Nova Science Publishers, 2009 (in press)
2. Vehicular ad-hoc Network: Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/VANET [3] "State of the art and research challenges for VANETs" Jakub Jakubiak, Yevgeni Koucheryavy [4] A. Stampoulis and Z. Chai, "A survey of security in vehicular networks.
3. "Secure VEhicular COMmunications,"http://www.sevecom.org/.
4. "Enhancing location privacy in wireless lan through disposable interface identifiers- a quantitative analysis," pp. 315–325, 2005.
5. K. Lee, S.-H. Lee, R. Cheung, U. Lee, and M. Gerla, "First experience with cartorrent in a real vehicular ad hoc network testbed," in 2007 Mobile Networking for Vehicular Environments, 2007, pp. 109–114.
6. Noncoperative Content Distribution In Mobile Infostations Networks- wing Ho, Yuen Roy D.Yates Siun-chuon Mau
7. Comparative Study of Data Dissemination Models of VANETs" Praveen Shankar, LIftode, Mobiquitous 2006.
8. M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications."
9. http://en.wikipedia.org/wiki/Intelligent_vehicular_ad-hoc_network
10. Rosslin Robles and Maricel O. Balitanas," A Review on Strategies to Optimize and Enhance the performance of WLAN and Wireless Networks" , IJMUE/vol2_no2_2007.
11. en.wikipedia.org/wiki/Intelligent_vehicular_ad-hoc_network
12. ArunkumarTangavelu "Location Identification and Vehicle Tracking using VANET (VETRAC)" IEEE-ICSN 2007, Feb 22-24, 2007pp 112-116
13. Tamer Nadeem, Pravin Shankar, Liviu Iftode "A Comparative Study of Data Dissemination Models for VANETs"