www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 3 Issue 5 may, 2014 Page No. 5970-5974*

# Location Privacy using Traffic-Aware Mix zones in Vehicular or Mobile Networks

***Anju Pathrose, T.Poornima***

, M.E, Anna University, Chennai, Maharaja College of Engineering and Technology,
Erode, Tamil Nadu, India
*rose18anju@gmail.com*

,Assistant Professor, Dept of CSE, Anna University,
Maharaja College of Engineering and Technology, Erode, Tamil Nadu. India
*tpoornivelt@gmail.com*

Abstract: **In VANET for the purpose of saftey, vehicles need to periodically broadcast safety messages providing precise position information to nearby vehicles. However, this frequent messaging (e.g., every 100 to 300ms per car) greatly facilitates the tracking of vehicles, as it success to eavesdrop the wireless medium. As a result, the driver's privacy can't be protected. In order to protect personal location information we proposes the mix zone concept. Cryptographic Mix (CMIX) protocol is used here to improve location privacy of Mix-Zone. We propose to do so using pseudonym changes and cryptography. The paper is concluded with an investigation based on current results of upcoming elements to be integrated in our secure VC architecture.**

Keywords: VANET, Cryptographic Mix zone,Vehicular Communication.

## 1. Introduction

VANET (Vehicular Ad-hoc Network) is a sub group of MANET which uses cars as mobile nodes to create a mobile network. The importance of VANET increases when the alert messages sent over the network can rescue us from accidents. The application also include warning about traffic congestion along the road course. For traffic security it is needed to interchange data over Vehicular Ad-hoc Networks (VANETs) . For example, in the eCall project, an emergency call made once in vehicle sensors detect that an accident has occurred . As lives could depend on this application, such information must be accurate and truthful,. To make an overview of the current status of security issues over the Vehicular Ad-hoc Networks, the communication models are identified from the security point of view.

Different classes of vehicles can move in VANETs, depending on traffic conditions (i.e., dense and sparse traffic), speed limits in particular roads (i.e., highways, rural roads, urban neighborhoods), and also typology of vehicles (i.e., trucks, cars, motorcycles, and bicycles). Vehicles in VANETs move at higher speeds (i.e., from 0 to 40 m/s), compared to traditional mobile nodes in MANETs,

Several applications are enabled by Vehicular Ad-hoc Networks (VANETs), mainly affecting road safety. Within this type of application, messages interchanged over the network have different nature and purpose. In Vehicular Ad-hoc Network, vehicles can communicate in several mechanism. In Vehicle-to-Vehicle communications (V2V), Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification messages can be exchanged. The CAM messages are beacon which are periodically sent. It consists of basic status information like speed, location, acceleration and vehicle identifier. Usually a vehicle's neighborhoods receives these messages. The DENM messages report information related with events and is sent on event detection. It is usually distributed to many vehicles over a large area and contains eventlocation and timestamp.

Moreover, vehicles can connect to an infrastructure-Vehicle-to-Infrastructure (V2I) to get some service. Infrastructure is mainly the Road Side Unit which can be located on road intersections. It provides location based and safety applications. But the V2V and V2I communications expose sensitive data to other vehicles, Eavesdroppers and to infrastructure. So our purpose is to provide anonymity by concealing idendity and location privacy so that the vehicle's position cannot be systematically recorded.

The proposal fits in this framework of pseudonymous authentication. The contribution is threefold. First, a protocol to create cryptographic mix-zones at road inter sections is proposed. This solution thwarts computationally bounded eavesdroppers while preserving the functionality of safety messages. Second, the location privacy achieved by combining mix-zones into of the degree of statistical dependence between the words.

## 2.PROPOSED WORK

### *2.1 PKI Communication*

In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA).The public key infrastructure is used to ensure user validity. The user identity must be unique within each CA domain. It has got two types of keys: a public key and a private key. Both the vehicles will have the two keys. The private key is known only to you while the public key is given to any vehicle that wants to communicate securely with it. To decode an encrypted message, a vehicle must use the public key provided by the originating vehicle and it's own private key.

Another major concern in security issues is authentication. To authenticate safety messages Digital Certificates are used. Digital Certificates are used. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.

Vehicles are equipped with Tamper Proof Devices (TPDs) that guarantee the correct execution of cryptographic operations and the non-disclosure of private keying material. TPDs come with their own battery and clock. Prior to entering the network, each vehicle *I* has to register with a Certification Authority.

Aim at increasing the adversary's workload to uniquely identify the author of an action, present a cryptographic technique to create anonymizing regions, that is, mix-zones in VNs. The idea for mix-zones is to prevent the adversary from accessing the content of (safety) messages, including the vehicle's signatures that are trivially linkable to the corresponding pseudonym, and thus be unable to connect two pseudonyms successively used by the same vehicle.

The aim of the mix zone model is to prevent tracking of long-term user movements, but still permit the operation of many short-term location-aware applications..

The effectiveness of anonymizing regions in providing location privacy depends on the density of vehicles and the unpredictability of their whereabouts. We propose to create mix-zones at predetermined locations and to force pseudonym changes to take place within those regions. Because the highest mixing of vehicles occurs at road intersections where the speed and direction of vehicles change the most (i.e., it is an appropriate mix context), we propose placing mix-zones at road intersections. We assume that all vehicles participate in the anonymization process at every road intersection. The figure 1. shows the concept.

### *2.2 Encryption And Decryption*

A certificate is attached to each message to enable other vehicles to verify the sender's authenticity. Vehicles are equipped with Tamper Proof Devices (TPDs) that guarantee the correct execution of cryptographic operations and the non-disclosure of private keying material. TPDs come with their own battery and clock. Prior to entering the network, each vehicle *I* has to register with a Certification Authority (CA) and preloads a large set of pseudonym.

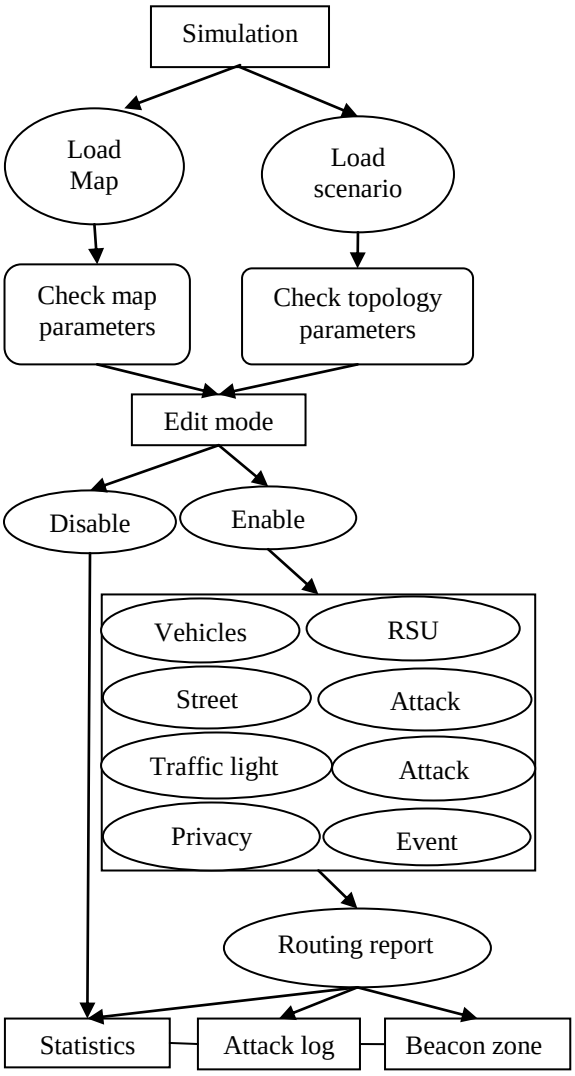


**Figure 1 Flow diagram of concept**

Pi,k, with k = 1…….. F, where F is the size of the pseudonym set. The CAs are fully trusted third parties and interoperable entities, operated by governmental organizations, that conform to privacy policies and keep the relation of the pseudonyms to the driver's real identity secret. In case of liability issues, this relation can be made public by law enforcement. For each pseudonym Pi,k the corresponding CA generates a unique public/private key pair (Ki,k Ki,k) and a corresponding certificate Cert I,k(Ki,k).1 Each vehicle sequentially updates its pseudonym at regular time intervals independently of other vehicles. Pseudonyms have a short validity period and cannot be reused.

In Vehicular Communication every message must be authenticated, to make sure for its origin and to control authorization level of the vehicles, to do this vehicles will assign every message with their private key along with its certificate, at the receiver side, the receiver will receive the message and check for the key and certificate once this is done, the receiver verifies the message Signing each message with this, causes an overhead, to reduce this overhead we can use the approach ECC (Elliptic Curve Cryptography), the efficient public key cryptosystem, or we can sign the key just for the critical messages only.

### *2.3 Mix ZRP protocol algorithm*

Step1: Key Establishment

Vehicles rely on the presence of RSUs at road intersections to initiate a Key Establishment mechanism and establish a symmetric key. RSUs advertise their presence by periodically broadcasting beacons.

$$Vi \rightarrow RSU \ : Request\ , T_S, Sign_i(Request, T_S), Cert_{i,k}$$

$$RSU \rightarrow v_i \ : EK_{i,k}\ (V_i, SK, T_S\ , Sign_{RSU}(V_i, SK, T_s)), Cert_{RSU}$$

$$Vi \rightarrow RSU \ : ACk\ , T_S, Sign_i(ACK, T_S), Cert_{i,k}$$

**The Key Establishment protocol.**

Ts is a time stamp, Sign() is the signature of the message and Cert is the certificate of the message sender.

The key establishment protocol is initiated when vehicle vi enters in the of transmission range of an RSU ie R Beacon. By checking the announced beacon the vehicle knows its own location and that of RSU .Thus it can determine whether it is within the mix-zone. If the vehicle vi is witin the mix zone it introduce one or if needed, several key request messages . The RSU replies with the symmetric key SK encrypted with the public key of vehicle vi and a signature. The vehicle receives this and decrypt it.All subsequent safety messages are encrypted with the use of this symmetric key until vi leaves the mix-zone. In case RSUs are co-located (i.e., their mix-zones overlap), vehicles are aware of all CMIX keys so that they can decrypt all messages. Alternatively, co-located RSUs could to use the same CMIX key.

Step2 :Key Forwarding

The extended mix-zone is the zone beyond the RCMIX range. The vehicle in that zone may be unable to obtain the key from the RSU directly; for example, they are beyond their transceiver's range.And also they cannot decrypt safety messages coming out of the CMIX. Such vehicles issue one or, if needed, several key requests to obtain the SK key with the help of vehicles already in the mix-zone which are aware of it.

Consider the example of Figure 2: vehicle v1 already knows the CMIX key and can forward it to v2. Hence, the RSU leverages on the vehicles in the mix-zone. In our example, when v2 enters the extended mix-zone, as soon as it receives an encrypted (intelligible) message, it initiates the broadcast of one or, if needed, several key requests. v1 eventually receives a key request from v2, and forwards it the symmetric key.

$$E_{K_{2,k}}(v_2, v_1\ , SK, T_S, Sign_{RSU}(V_1, SK, T_s))$$

For validating the transmitted symmetric key the timestamp and signature from RSU are used. Only after entering the mix-zone (RCMIX) vehicles in the extended region will encrypt their safety messages. The entire above message is in addition signed by v1.

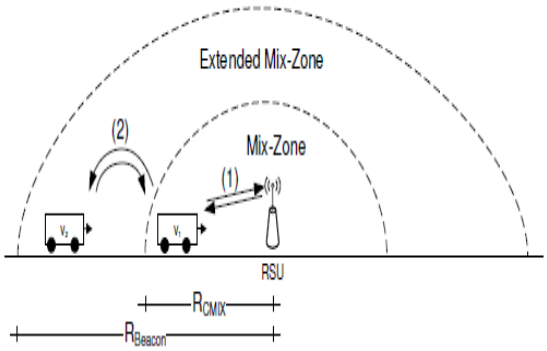


**Figure 2 Extended Mix-zones. (1) *v*1 uses the Key Establishment to learn the symmetric key. (2) *v*2 uses the Key Forwarding protocol.**

Step3 :Key Update

For renewing or revoking CMIX symmetric keys we propose a Key Update mechanism . The RSU determines when to initiate the process and do the key updates. Key updates occur only when the mix-zone is empty and the key transport and key forward protocols are used by the vehicles to obtain new keys. The CA obtains the new symmetric key from the RSU over a secure channel, to satisfy the liability requirements (i.e., possibly, decrypt safety messages in the future). If key up dates are asynchronous across different base stations the robustness will be great. As frequent updates can cause additional overhead, there would be a trade of between security and cost.

## 3 .RELATED WORK

The background to the VANET privacy problem have discussed in several papers and the merits of the pseudonymous authentication solution [6] [3] [2].The primary aim of vehicular networks is to secure user identification and location privacy. For that public key infrastructure in accordance with Anonymous public keys are used like explained in [7] and [10].With the aid of the protocol analysis tool ProVerif [4] certain scenarios are discussed in which CMIX protocol can prevent privacy from being achieved. They include a second necessary condition for privacy that that vehicles do not change pseudonym too early or too late.

To service a query for finding the nearest shopping mall or gas station, the Location Based Service (LBS )should be used. It is described in [6].For providing a requested service this application obtain and make use of the most recent location of a mobile node.The co-operative driving[6] is also achieved where a very short separation is maintained each other between equipped vehicles.

Group navigation of vehicle [1] concept can be used to avoid unauthorized tracking of vehicles. By location tracking the location history of the vehicle user can be accumulated over time. And , the visited locations of the vehicle can be associated with places of interest by combining it with geographical maps and additional information. Thus the personal interest of the vehicle user can be inferred and profiled. These attacks present threats to the location privacy of the vehicle user [7].

## 4.IMPLEMENTATION

### *4.1 Vehicular networks*

Let a suitable public key infrastructure is available in VNs and that the messages are properly signed to ensure the liability of their sender in case of an accident. Vehicles are equipped with Tamper-Proof Devices (TPDs) that guarantee the correct execution of cryptographic operations and the non-disclosure of private keying material. TPDs come with their own battery and clock. Prior to entering the network, each vehicle I has to register with a Certification Authority (CA) and preloads a large set of pseudonyms Pi;k, with k = 1; :::; F, where F is the size of the pseudonym set. The CAs are fully trusted third parties operated by governmental organizations. Their duty is to conform to privacy policies and keep the relation of the pseudonyms to the driver's real identity secret. In case of liability issues, this relation can be made public by law enforcement. For each pseudonym Pi;k the corresponding CA generates a unique public/private key pair (Ki;k;K¡1 i;k ) and a corresponding certificate Certi;k(Ki;k).1 Each vehicle sequentially updates its pseudonym at regular time intervals independently of other vehicles. Pseudonyms have a short validity period and cannot be reused.

### *4.2 Threat Model*

An external adversary installs its own radio receivers near the road network and passively eavesdrops vehicle safety messages. Outside the range of its radio receivers, the adversary cannot overhear transmissions. Thus, its strength depends on the number of its eavesdropping devices. A global adversary has a complete view of the monitored network. Such an adversary can be put in place by exploiting already deployed 802.11 networks. For example, wireless social communities (e.g., FON [10]), or WiFi operators (e.g., Google) provide low cost wireless internet connectivity via WiFi networks in cities. With minor software or hardware modifications, this infrastructure can eavesdrop VN communications.

On the other hand, setting up a network of internal eaves droppers would be much harder. The adversary would need to obtain legitimate devices, e.g., vehicles equipped with transceivers. The use of a TPD prevents adversaries from compromising cryptographic material. However, the VNO, which is a partially trusted third party, could be enticed to passively monitor the position of vehicles. We do not consider this type of adversary. We assume instead in this paper that the VNO assists in setting up privacy protection mechanisms.

### *4.3 Cryptographic Mix-zones*

Anonymous systems, as described, aim at increasing the adversary's workload to uniquely identify the author of an action. In this section, we present a cryptographic technique to create anonymizing regions, that is, mix-zones in VNs. The idea for mix-zones is to prevent the adversary from accessing the content of (safety) messages, including the vehicle's signatures that are trivially linkable to the corresponding pseudonym, and thus be unable to connect two pseudonyms successively used by the same vehicle.

The effectiveness of anonymizing regions in providing location privacy depends on the density of vehicles and the unpredictability of their whereabouts. We propose to create mix-zones at predetermined locations and to force pseudonym changes to take place within those regions. Because the highest mixing of vehicles occurs at road intersections where the speed and direction of vehicles change the most (i.e., it is an appropriate mix context), we propose placing mix-zones at road intersections. We assume that all vehicles participate in the anonymization process at every road intersection.

The CMIX protocol requires the exchange of two messages. One or several key request messages are sent until either an RSU or a vehicle receive it. Such transmission overhead can be kept low: in a dense traffic scenario, one key request should success before receiving a reply, whereas in a low-density scenario the message overhead has low impact. When a key request is broadcasted, potentially every vehicle in the transmission range could send back a key re- ply. To avoid such reply coding, a number of mechanisms can be used (e.g., random backoff mechanism); we will evaluate those in future work. Upon receipt of the mix-zone key, the vehicle sending the key request acknowledges the acquisition of the key, to prevent additional neighboring vehicles from forwarding again the key.

## 5.CONCLUSION

Providing location privacy to users is one of the important issues that must be addressed in Vehicular Ad-Hoc Networks. Our main goal is to develop a security architecture for VANETs that balances security requirements of all participants and also try to identify and - if necessary - develop feasible mechanisms that fit in this architecture. In this paper It is addressed by using cryptographic mix-zones. A cryptographic technique to create anonymizing regions, that is, zones in VNs. The idea for mix-zones is to prevent the adversary from accessing the content of messages, including the mobile's signatures that are trivially linkable to the corresponding pseudonym, and thus be unable to connect two pseudonyms successively used by the same mobile.

Like other anonymous routing protocol, this work is also not devoid to all attack. Future works lies in reinforcing mix zones in an attempt to thwart stronger, active attackers and demonstrating comprehensive results.

## REFERENCES


[1]Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran," AMOEBA: Robust Location Privacy
Scheme for VANET," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, vol. 25, no. 8, october 2007

[2] Balaji Palanisamy, Ling Liu, Kisung Lee, Aameek Singh† and Yuzhe Tang," Location Privacy with Road network Mix-zones," College of Computing, Georgia Tech †IBM Research - *Almaden*

[3] Julien Freudiger, Maxim Raya, Márk Félegyházi,Panos Papadimitratos and Jean-Pierre Hubaux," Mix-Zones for Location Privacy in Vehicular Networks**,**" EPFL, Switzerland
firstname.lastname@epfl.ch

[4] Morten Dahl, St´ephanie Delaune,and Graham Steel," Formal Analysis of Privacy for VehicularMix-Zones," Department of Computer Science, Aalborg UniversityLSV, ENS Cachan & CNRS & INRIA Saclay ˆIle-de-France

[5] Mrs. Arzoo Dahiya, Mr. Vaibhav Sharma,"A Survey On Securing User Authentication in Vehicular Ad-hoc Networks," Computer Science & IT Department, Institute of Technology and Management Sector-23 A, Gurgaon-122017

[6] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura and Kaoru Sezaki," CARAVAN: Providing Location Privacy for VANET,". In 3rd workshop on Embedded Security in Cars (ESCAR 2005), 2005.

[7] Maxim Raya and Jean-Pierre Hubaux,"The Security of Vehicular Ad Hoc Networks," In Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), November 2005.

[8] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, Fellow, IEEE "An Identity-Based Security System for

User Privacy in Vehicular Ad Hoc Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 9, SEPTEMBER 2010
[9] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung," Wireless Location Privacy Protectionin Vehicular Ad-Hoc Networks," Department of Electrical and Computer Engineering
The University of British Columbia, Vancouver, BC, Canada, V6T 1Z4
E-mail: {joohans, vincentw, vleung}@ece.ubc.ca
[10] A. Rao, A. Sangwan, A. Kherani, A. Varghese, B. Bellur, and R. Shorey." Secure V2V Communication With Certificate Revocations," In proceedings of the IEEE Infocom 2007, MOVE Workshop.
[11] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," IEEE Commun. Mag., vol. 46, no. 11, pp. 100–109, Nov. 2008.
[12] M. Raya, P. Papadimitratos, V.D. Gligor, and J.-P. Hubaux, "On datacentric trust establishment in ephemeral ad hoc networks," in Proc. 27th Conf. IEEE INFOCOM, 2008, pp. 1238–1246.
[13] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in Proc. 1st ACM Int. Workshop VANET, New York, 2004, pp. 29–37.
[14] J. Petit, M. Feiri, and F. Kargl, "Spoofed data detection in VANETs using dynamic thresholds," in Proc. IEEE VNC, Nov. 2011, pp. 25–32.
[15] S. Dietzel, J. Petit, F. Kargl, and G. Heijenk, "Analyzing dissemination redundancy to achieve data consistency in VANETs (short paper)," in Proc. 9th ACM Int. Workshop Veh. Inter-Netw., New York, 2012, pp. 131–134.
[16] R. K. Schmidt, T. Leinmueller, E. Schoch, A. Held, and G. Schaefer, "Vehicle behavior analysis to enhance security in VANETs," in Proc. 4th IEEE V2VCOM, Eindhoven, The Netherlands, 2008.
[17] B. Bako, F. Kargl, E. Schoch, and M. Weber, "Advanced adaptive gossiping using 2-hop neighborhood information," in Proc. IEEE GLOBECOM, 2008, pp. 1–6.
[18] L. Wischhof, A. Ebner, and H. Rohling, "Information dissemination in self-organizing intervehicle networks," IEEE Trans. Intell. Transp. Syst., vol. 6, no. 1, pp. 90–101, Mar. 2005.