Privacy Protection with Dynamic Pseudonym-based Multiple Mix-Zones Over Road Networks

Article · April 2017

CITATIONS
0

READS
56

7 authors, including:

Imran Memon
Zhejiang University
85 PUBLICATIONS **453** CITATIONS
SEE PROFILE

Asma Zubedi
Beijing University of Posts and Telecommuni…
9 PUBLICATIONS **58** CITATIONS
SEE PROFILE

Jichao Jiao
Beijing University of Posts and Telecommuni…
34 PUBLICATIONS **70** CITATIONS
SEE PROFILE

Privacy Protection with Dynamic Pseudonym-Based Multiple Mix-Zones Over Road Networks

Qasim Ali Arain[*1] , Zhongliang Deng [1] , Imran memon[2] , Asma Zubedi[1] , Jichao Jiao[1] , Aisha Ashraf[3] , Muhammad Saad Khan[1]

[1] Beijing University of posts and Telecommunication Beijing China
[2] College of Computer Science, Zhejiang University, Hangzhou 310027, China
[3] Department of Software Engineering Mehran UET Jamshoro.
[*] The corresponding author, e-mail: Qasim_ali_arain@yahoo.com

Abstract: In this research we proposed a strategy for location privacy protection which addresses the issues related with existing location privacy protection techniques. Mix-Zones and pseudonyms are considered as the basic building blocks for location privacy; however, continuously changing pseudonyms process at multiple locations can enhance user privacy. It has been revealed that changing pseudonym at improper time and location may threat to user's privacy. Moreover, certain methods related to pseudonym change have been proposed to attain desirable location privacy and most of these solutions are based upon velocity, GPS position and direction of angle. We analyzed existing methods related to location privacy with mix zones, such as RPCLP, EPCS and MODP, where it has been observed that these methods are not adequate to attain desired level of location privacy and suffered from large number of pseudonym changes. By analyzing limitations of existing methods, we proposed Dynamic Pseudonym based multiple mix zone (DPMM) technique, which ensures highest level of accuracy and privacy. We simulate our data by using SUMO application and analysis results has revealed that DPMM outperformed existing pseudonym change techniques and achieved better results in terms of acquiring high privacy with small number of pseudonym change.

Keywords: road network; multiple mix-zones; location privacy

I. INTRODUCTION

The advent of mobile communication and ubiquitous computing has extended the opportunities for users to make life easier by accessing vast information through location based services. However, when the users get registered with these services, they may be exposed to the threat of information disclosure [1,2]. Personal data privacy has not been a critical problem but due to the expansion of location based services, an adversary can track a user's location by accessing his information. As a consequence, location privacy of user becomes a challenge [3,4]. The private information of a user, that is recorded during his visit to a hospital, library, and social networking website or while driving on a road becomes an invasive catalogue of data. Despite, it remains a strenuous task to achieve the desired level of protection by using a single mix-zone [5]. Consequently, it gives the opportunity to any malevolent adversary to track the user and may cause harm.

In the last decade, various pseudonym changing techniques for the protection of location privacy in VANETS have been proposed [6,7,8 9,10,11]. This can be achieved

Received: Feb. 4, 2016
Revised: Sep. 15, 2016
Editor: Shangguang Wang

In this paper the authors proposed an advanced method to improve user privacy in terms of dynamic pseudonyms, while focusing on multiple mix-zones over road networks.

by changing the identifier of a target vehicle called the pseudonym that is chosen randomly. However this mechanism is performed by location server, therefore, by executing pseudonym change, the services from main server will be disturbed which is the cause of overhead in the network [12,13,14]. Despite, most of the current pseudonyms change mechanism ignores this crucial aspect15,16,17,18] but the problem persists because if single vehicle changes its pseudonym, it can be tracked easily by an attacker [19,20,21,25,26,27]. Moreover, it has been further investigated that when multiple vehicles are inside mix-zone, they may change their pseudonyms [23,24]. On the contrary, an attacker can easily discover mix-zones because, mix-zones are mostly, statically determined [25, 26]. So, this concept led to further research and explored the idea of dynamic mix zone [9, 26,27,28,29] which emphasizes on the technique of pseudonym change with dynamically determined mix-zones. In [14] game theory approach has been proposed for non-cooperative location privacy. In this approach, selfish vehicles alter their pseudonyms when they have maximum payoff but it fails in the situations, where few vehicles may not change their pseudonym if they have achieved satisfactory level of location privacy. As a result, in most of the cases, the vehicles whose pseudonyms have expired may not have sufficient number of other vehicles willing to change their pseudonyms. This, in turn, adversely affects the location privacy provided to the vehicles in need.

After detailed analysis of existing limitations, we presented a protocol that will generate some inducement for vehicles to change their dynamic pseudonyms inside as well as outside the mix-zone. Our proposed model comprises of following important factors:

(i) We have introduced a reputation method that gradually encourages each vehicle to change Dynamic Pseudonym Multiple Mix-zones (DPMM) within the mix-zone as well as outside the mix-zone.

(ii) We further propose dynamic pseudonym multiple mix-zones (DPMM) generation with privacy protection that comprises of various parameters for defending against constant attacks.

(iii) The simulation results indicate that the proposed technique provides better results, acquiring high rate of protection with reduced number of changes in pseudonyms, along with presenting the best performance.

II. System Model

2.1 General idea description

We have proposed a Dynamic Pseudonym Multiple Mix-zone model (DPMM) for mobile travelers over Road networks. There are four main entities that can be shown in figure 1, i.e. mix zone, reported server, road side unit and vehicles. Mix zone is an area where vehicles change their pseudonyms; however vehicles can change their pseudonyms inside as well as outside mix zone. Reported server is an entity which allows communication between RSU and vehicle and it is also responsible to authenticate vehicle over the road network. Moreover, vehicles are connected to reported server (RS); they may change pseudonyms even when they are outside mix-zone. RSU is a computing device located on the road sides, which can provide connectivity to the vehicles. So, our proposed model based on secure communication between these four entities as shown in figure 1.

2.2 Assumptions

In this research model, we have proposed a protocol and have assumed that each vehicle has a unique ID (identity information in road network). This ID is only shared with reported server (RS). We also assumed that RS1, RS2… RSn all are connected with main RS servers and main RS verify each unique ID information and provide information to multiple reported server (RS), which is used for requesting a change in pseudonyms when vehicle travels inside or outside a mix-zone. It is further assumed that every vehicle is authenticated by a private or public key. This

key allows a vehicle to acquire its pseudonym and its RS information from reported server. Moreover, mix-zone and reported server are trusted entities, while RSU (Road side unit which is providing connectivity between multiple RSUs and also communicate with reported server) is not a trusted entity. Under such circumstances, a reported server is responsible to control vehicles. RS information and public keys, both are available at reported server. Reported server broadcasts a public pseudonym for each vehicle which comes under its range or detected over road network. The availability feature of RS is almost perfect. Additionally, it has the information of RS private IDs and encrypted information of public keys associated with every vehicle. Thus, RS will acquire a vehicle's public key and frequently update it.

2.3 Model description

(1) In our first approach, we have proposed that every vehicle gets associated with RS, where RS allocates a virtual identity and a secret pseudonym. The virtual ID (dummy identity of vehicle user instead of using real identity) is a node identity for vehicle user which is 128-bit address used for both node identity and locator. The virtual ID is pre-defined and randomly assigned by the main reported server. This ID is permanent and thus, no longer bound to the main reported server and/or locations. Once a vehicle receives a virtual identity and a private pseudonym, it will resend it to reported server which, in turn, broadcasts this new generated RS information. Hence, vehicle encryption includes public pseudonym, its virtual identity and timespan of RS information. Time span of RS information can be defined as time which is required for a vehicle to travel at a regular speed to cover distance between two reported servers. During this process, vehicle sends its virtual identity to RS, before its certificate expires. RS will resend newly generated private pseudonym to vehicle when it receives virtual identity of vehicle, while at the same time, it will update reported server regarding the vehicle's information. Hence, reported server will broadcast certificate. In this approach, vehicles on road are identified by their virtual identity while pseudonyms allow them to communicate. However, in this approach only RS will communicate with road side unit (RSU) .The number of road side unit (RSU) may communicate with multiple reported servers which are installed within the infrastructure. Therefore, the capacity of multiple reported servers and number of vehicles to communicate with an infrastructure depends upon the radio coverage of existing RSUs in the nearby area. The bandwidth required to send a request and receive response of pseudonym will be analyzed in section III and its parameter is defined in Table 1.

2) In our second approach, we have proposed that every vehicle has both its private and public key. As the vehicle acquires RS public key, it will be authenticated on road network by encrypting its private keys and public keys with RS public key. Hence, vehicle pair keys (i.e. private/public) get registered with RS and in turn, RS will send a set of information to vehicle by encrypting them with vehicle public key. This information contains a message that allows vehicles to create their private pseudonym and certificate. So based on this, when a vehicle receives a set of information, it creates a certificate and a private pseudonym. Once it is done, RS information

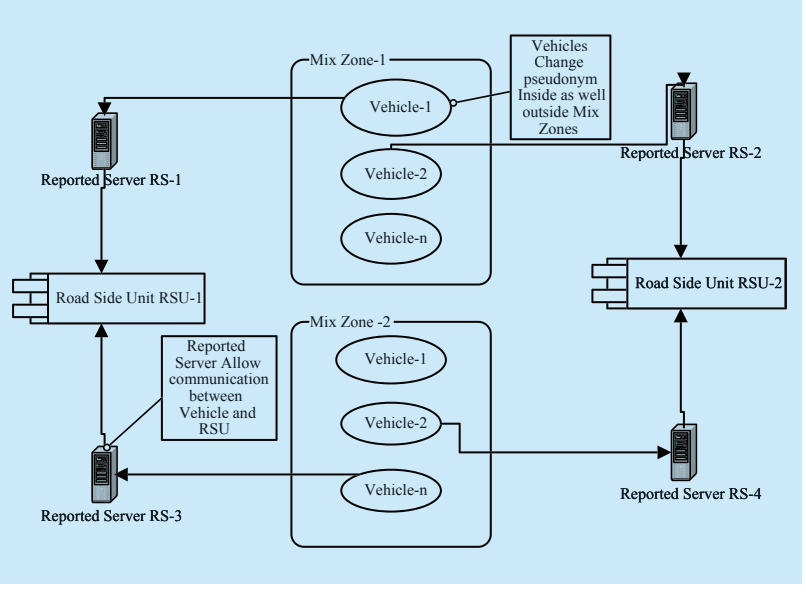

Fig. 1 *Basic work Flow illustration of DPMM*

Table I *Notation description*

Notation	Description
V_{id}	Vehicle's identity.
V_{pKey}	Vehicle's private. Key
V_{pbKey}	Vehicle's public key.
RS	Report server
Vpr	Vehicle's private pseudonym.
V_{vid}	Vehicle's virtual identity.
V pseudRSinf	Vehicle's pseudonym and Report server information.
RpKey	RSU's private key.
RpbKey	RSU's public key.
ERpbKey(V_{id})	Asymmetric encryption function at encrypts the vehicle identity with RSU public key.
EV $_{id}$(Vpseudo+V_{vid})	Symmetric encryption function that pseudonym and its virtual identity with the real identity of the vehicle.
ERpbKey(VprKey + V pbKey)	Asymmetric encryption function public key with RSU public key.
EVpbKey(V pseudRSinf)	Asymmetric encryption function that encrypts the set of information (which permit at the vehicle to generate its pseudonym and certificate) with its public key
Br(V_{RSinf})	Broadcast the vehicle certificate.
EVid(V_{vid})	Symmetric encryption function that encrypts the vehicle virtual identity with its real identity.
$EV_{id}(v'$ prpseudo+$v'_{vid})$	Symmetric encryption function that encrypts the new private pseudonym and virtual identity of the vehicle with its real identity.
v'_{RSnew}	Vehicle's new RS information
Br(v'_{RSnew})	Broadcast the new RS information

First Approach: Steps are as Follows

1: RS broadcasts periodically its public key.
2: Vehicle sends to RS a ERpbKey(Vid) message.
3: RS sends to the applicant vehicle a EVid(V prpseudo + V vid) message.
4: RS sends to RSU aV RS inforamtion message.
5: RSU broadcasts V RS inforamtion message..
6: Vehicle sends a EV id(V vid) message to the RS.
7: RS delivers a EV id(v'prpseudo + v'vid) message to the vehicle.
8: RS sends to RSU a V'RS inforamtion message.
9: RSU broadcasts v'RS inforamtion message

Second Approach: The steps are as follows:

1: RS broadcasts periodically its public key.
2: Vehicle sends to RS a ERpbKey(V prKey + V pbKey) message.
3: RS sends to the applicant vehicle a EV pbKey(V pseudRsinf) message.
4: Vehicle generates its private pseudonym and RS information.
5: Vehicle broadcasts its new RS information.
6: Vehicle updates its private pseudonym and new RS information.
7: Vehicle broadcasts the new RS information

will be broadcasted. As soon as RS information expires, it will generate a new private pseudonym that will be broadcasted. Pseudonyms are the only way to identify vehicles by using this approach. However, vehicles in second method are free to communicate their private pseudonyms and certificates, once they have been validated by RS.

The RSUs are scattered equidistantly to measure expiration time of certificates and private pseudonyms. Consider "d" as a distance between each road side unit and communication range of each road side unit. Moreover, maximum and minimum speed on road are represented by V_{max} and V_{minax}, respectively. It is assumed that there must be at-least two vehicles which may travel at an average speed. The main goal of our approach is to allow at least two vehicles to acquire pseudonym on road during same time interval. It is denoted by $V_m = (V_{max} + V_{min})/2$. The ratio determined between distance "d" and "V_m" will be the expiry time "t" of certificate and private pseudonym, which is represented by $t = d/V_m$. The communication range of each road side unit is equal to "d" as mentioned previously. Therefore, vehicle at any speed can communicate with at least one road side unit and is allowed to change its pseudonym at least once while on the road.

Location privacy is an important aspect to consider in road networks, according to this, vehicles have to disseminate information to other vehicles which are coming under their premises for safety application or accident warning. To mitigate and manage an attacker from tracking a vehicle's trajectory, it is required that vehicle must change their pseudonym at multiple time and location, however it is evident from the discussion that existing methods regarding pseudonym change are not capable enough for desired location privacy. Therefore, it is very easy for an attacker to quantify the vehicle's movement by using relative coordinates, which in turn, manipulate vehicle's location privacy. Moreover, due to less number of pseudonyms stored inside vehicle and bottleneck occurred due to high frequency

of updating pseudonym. It is therefore evident that some selfish vehicles inside mix zone may not cooperate and do not proceed to alter their pseudonym when current strength of location privacy is larger or equivalent to the minimum level of location privacy.

To cope with this critical (to location privacy) issue, we have proposed reputation based technique, which enable vehicles to cooperate for pseudonym change. Moreover, strength of location privacy increases, as number of vehicles cooperates, and the value of that increase depends upon the number of vehicles that will be cooperating. We have proposed that vehicle will change their pseudonym when they are inside as well as outside mix zone. It has been already mentioned in [26, 27, 25] the strength of the location privacy is directly proportional to number of vehicles that are cooperating, however, when number of vehicles cooperate, they will change their pseudonyms inside and outside of mix zone causing location privacy to increase. Let us consider the following example: if there are 10 vehicles entering the mix zone and four of these vehicles change their pseudonym inside mix zone, then it is very easy for an attacker to calculate entrance as well as exiting time and the related information. So, it is clear from above discussion that if less number of vehicles changes their pseudonym then location privacy decreases. But, if the number of vehicles changing their pseudonyms are large while entering and exiting mix zones i.e. 10 then it is very difficult to launch an attack. Also, some selfish vehicles do not change their pseudonyms so their strength of location privacy decreases. Overall conclusion is that, strength of the location privacy is proportional to number of vehicles that are cooperating. The strength of location privacy of DPMM improves because large numbers of vehicles are cooperating and changes their pseudonyms in order to increase their reputation. However, curves in EPCS (Efficient Pseudonym Changing Schemes for Location Privacy Protection) [25], RPCLP (Reputation-based Pseudonym Change for Location Privacy in Vehicular Networks) [26] and MODP (Mix-zones Optimal Deployment for Protecting location privacy) [27] schemes have small fluctuations. This is because these three schemes do not have any incentive policy to encourage vehicles to cooperate for pseudonym changes.

2.4 Attacks in multiple mix-zones over road networks

In the following section, we shall discuss the possible attacks on the road network.

(1) Fabrication Attacks: In this type of attack, an adversary may penetrate some malicious information into the network. When appropriate entity in the network would receive unauthorized packet, it can be misled to some anonymous destination. Moreover, It is very easy for an invader to initiate this type of attack by penetrating vague information into the network, however it is also possible that sender might assume that it is somebody else. These might include fabricate message and warning certificate identities [30, 31, 35]. According to this construct, drivers manipulate messages by using broadcast method and then execute the attack by sending information into the network. Message Fabrication has two possible forms. According to first technique incorrect information related to attacker's ID, speed and position of vehicle has been transferred to nearby vehicle or RSU. According to second construct, it has been assumed that, attacker will act as an emergency vehicle, in turns he/she can drive at a higher speed [32]. Our system avoids this type of attack because of secure communication system architecture and RS server. Secondly, we cloak synchronization (between nodes) and IP filtering in our system.

(2) Message Suppression Attacks: In this type of attacks, an adversary might drop down some critical information or some message which is sent to the receiver or hold that information to be used for later time. In road networks, this may create a very critical issue, like the information regarding the accident may not reach to the user in time. In case of any mishap, the information regarding that

incident will not immediately be propagated to the insurance authorities. Moreover, these messages might contain very important information for the receiver. By acquiring these packets, attacker can manipulate and use them again at some other time. The main reason behind such type of attacks would be to handicap registration and insurance authorities from learning about road accidents and to generate delay in disseminating collision information to RSU. It is evident from the discussion that, attacker may restrict any message related to congestion warning and might use it at some other time , in response vehicles do not receive the warning and can be forced to wait in the traffic [33,34].

(3) Alteration Attacks: Adversary, in such attacks, tries to change existing information by using delaying tactics or changing the actual information about the entry of vehicle that has been communicated. In such scenario, an adversary may alter the message by informing its neighbor vehicles on the road network that the road is clear but on the contrary, the road is blocked [30,36,37].

(4) Denial of Service Attacks (DOS): These are very popular security threats in the communication network. In this type of an attack, the attacker acquires the control of the resources, blocking the channel used by vehicular network. This will restrict the information from arriving safely and timely at final destination. Hence, these types of attacks may hinder drivers who are dependent upon application's information. In order to avoid such circumstances, the driver may switch between multiple channels or technologies if available like Bluetooth, LTE Wifi and DSRC [30, 38, 39].

(5) Replay Attacks: An adversary attacks by repeating the communication of a message that has been received earlier. By doing this, he will take the advantage of current situation and plan some critical attacks. However message does not contain any time stamp value or sequence number information. It is well known fact that, keys can be reused and it might be possible to re send these stored messages with the same key by adding malicious information into the system without any detection. Moreover to avoid such type of attacks each and every packet must be authenticated, not only just encrypted and packets should have some timestamp information. Such type of attacks may launch to confuse the authorities to prevent identification of vehicles in hit-and-run incidents [33, 34].

Table II *Simulation Parameters*

Parameters	Value
Northwest Atlanta region Map	14km x12 km
Number of RSU	50
Simulation time	10 min
No of vehicles	10,000
Vehicle speed (m/h)	100–250
Bit rate	6Mbps
MAC protocol	IEEE 802.11
RSU Communication range	500m
Vehicle communication range	200m
Road Junctions	10,000
Max. transmission range	10ms
Min. transmission range	2ms
Routing protocol	AODV
Number of Mix-zones	500
Number of Road junctions	6831
Number of Road segments	9187
Mobility Model	Random Rnet Router

III. Experiments and Evaluation

3.1 Experiment setup

We have evaluated our proposed method with SUMO simulator [22-24], and real map Northwest Atlanta region Map is used. We have based our analysis covering a large area of 14 km x 12 km and over 10,000 vehicles moving at varying speed. The simulations have been run five times, moreover network parameters are set as shown in Table 2.

3.2 Performance evaluation

The simulation results have shown that vehicles passing through multiple mix-zones have changed their pseudonyms dynamically as depicted in fig.2 Five different numbers

of mix-zones and their data mechanisms corresponding to dynamically changing pseudonyms have been considered respectively. It is worthy to note here that, due to dynamically changing pseudonyms in y-axis as shown in figure. 2, it is clear that DPMM is a better technique in terms of dynamically changing pseudonyms as compared to EPCS (Efficient Pseudonym Changing Schemes for Location Privacy Protection) [25], RPCLP (Reputation-based Pseudonym Change for Location Privacy in Vehicular Networks)[26] and MODP (Mix-zones Optimal Deployment for Protecting location privacy)[27].In particular, DPMM always performs the best. As a matter of fact, pseudonym-change badly influences communication performance. If a pseudonym change interval is longer, then the privacy exposure time increases. However, if pseudonym-change interval is shorter, then overhead increases because of frequent pseudonym change. Therefore, an algorithm is required that finds an optimal pseudonym-change interval for making a balance between communication overhead and location privacy.

The average strength of location privacy for a number of vehicles, moving in SUMO simulation over Northwest Atlanta region map is shown in figure 3. The average strength of location privacy achieved by DPMM and EPCS is higher than RPCLP and MODP schemes, where certain selfish-vehicles inside mix-zones possessed greater location privacy thus, refusing to change their pseudonyms. The average strength of location privacy in DPMM scheme is greater when compared with other three schemes because it causes DPMM to make vehicles change their dynamic pseudonyms when they pass inside and outside the mix-zones. We conclude that average strength of location privacy maintains a certain value when numbers of vehicles increase. We further measured distance between two nodes to calculate the average location strength by using equation 4.

$$Dist_{avg}(i,j) = \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} \left| L_i(K) - L_j(K) \right| \quad (1)$$

Delay Characteristics

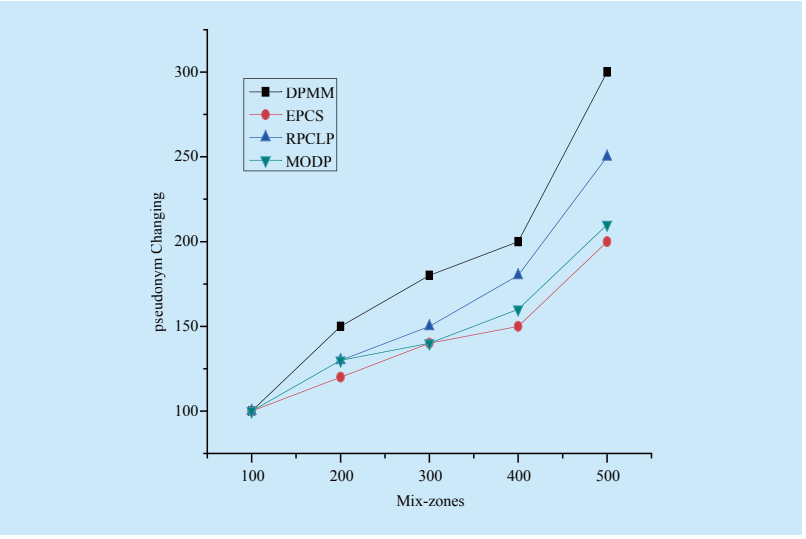

Fig. 2 *Dynamic pseudonym changing*

In vehicle networks, mostly delay characteristics depend upon the road intersection. The adversary formulates road intersections with normal distributions. The delay characteristic has been investigated by using normal distribution that would use trajectory of vehicle on intersection. For example, if f is number of road segments that meets at an intersection, and we have f = 4; for vehicles arriving from u1, their delay characteristic is represented as:

$$P_{u1}, e^{i}(t) \sim (\mu_1, i, \sigma_1, i) \quad (2)$$

Where I = 1…… f and e1, e2, e3 and e4 indicates the direction respectively.

Packet delivery Ratio

The packet delay is the time packet takes to achieve the destination after it leaves the source. The average end to end delay Xavg can be calculated by equation given below where Wr is the emission instant of the package and Wt is the reception instant of the package.

$$X_{avg} = \sum_{j=1}^{P_r} (W_r - W_t) / P_r \quad (3)$$

Location privacy inside mix-zone and outside mix-zone is represented by Ħ, however, it increases when vehicles cooperate. The strength of location privacy is directly proportional to the number of vehicles that are cooperating inside and outside mix-zone. Hence, after n number of rounds, final strength of location privacy is determined by:

$$\hat{H}_H^n = \sum_{y=1}^{n} W_\tau^y / A_\tau^y \quad (4)$$

The average strength of location privacy and dynamic pseudonym's lifetime is calculated for various seconds as shown in figure 4. The average strength of location privacy achieved by RPCLP scheme is highest as compared to DPMM and other two schemes. However, our DPMM scheme statistics still satisfies location privacy. Figure 4 shows that

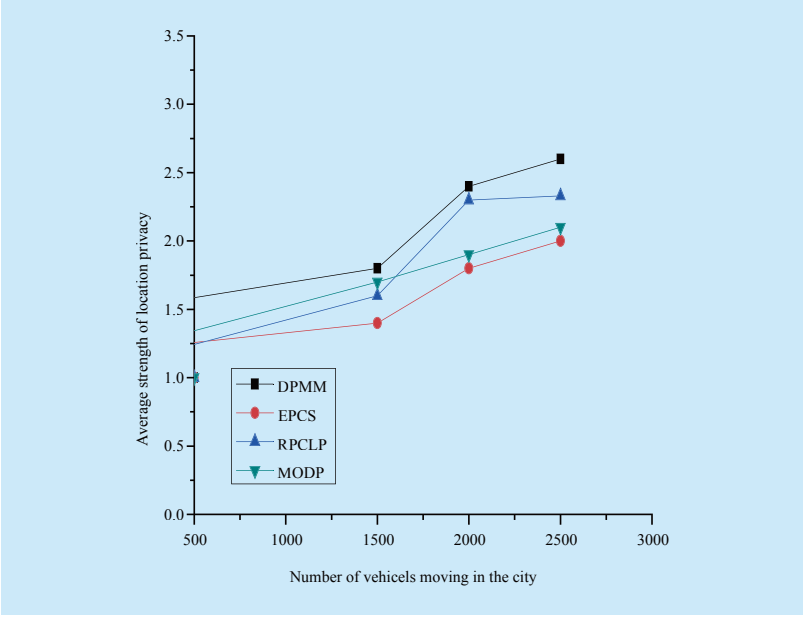

Fig. 3 *Location privacy*

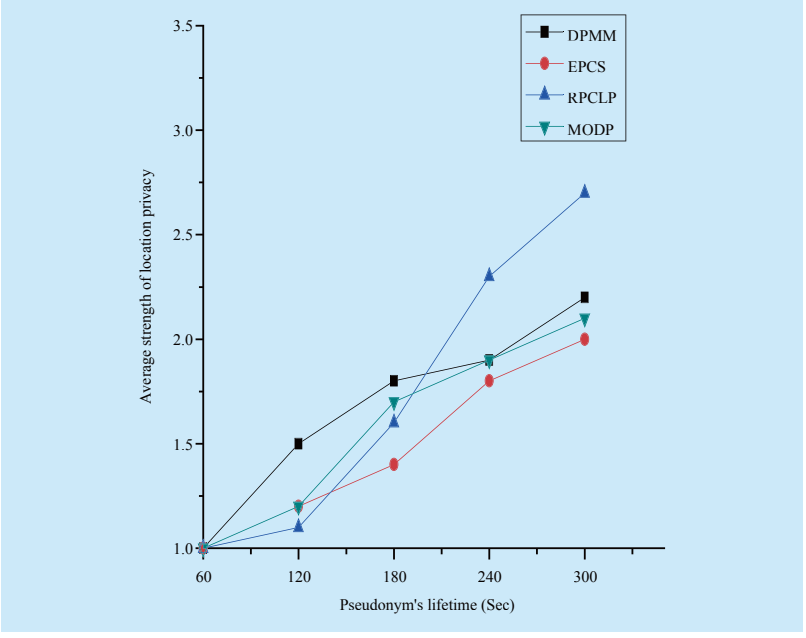

Fig. 4 *Average strength of location privacy*

the average strength of location privacy maintains a certain value with increase of dynamic pseudonym's lifetime whereas; dynamic pseudonym's lifetime has little impact on average strength of location privacy.

We have performed our simulations on several vehicle densities as shown in figure 5. It is evident from the experiments that with a rapid increase in number of vehicles, communication range decreases greatly as compared with the methods such as EPCS, RPCLP and MODP schemes in terms of time delay and throughput. However, with a shorter time delay, greater will be the DPMM scheme. We have compared figure 5 (a and b) for time delay, (c with d) for throughput and finally (e with f) for packet delivery ratio, and concluded that DPMM has outperformed EPCS, RPCLP and MODP in terms of time delay, through put and packet delivery ratio. Moreover, in figure 6 (a) and (b), we have observed

probability changing pseudonyms inside mix zone and outside mix zone. It is evident from the performed experiments that DPMM scheme performs better in terms of number of vehicles verses probability changing pseudonym.

Additionally, as the number of vehicles increases, DPMM will give the better results as compared to other three schemes. Finally, it has been evident from figure. 5 and 6 that better results are achieved when traffic on road becomes heavier and hence, throughput can get a greater value.

Probability changing the pseudonyms

$\phi(v)$, is the probability that vehicle v is connected to RS and passed through number of mix-zones during the same interval. $\Psi(P_V)$ is the probability that a vehicle changes pseudonym inside and outside mix-zones while going through the road it has chosen to have pseudonym (P_V).

The number of mix-zones in the road system is given by graph and edge (G, E).

The maximum number of vehicles connected which pass through mix-zones on the road system are denoted as mix-zones_r and the dynamic pseudonyms are denoted as mix_rdpvt.

Here, we define:

$G([PV1,\ldots.,PVC])$ to be the set of dynamic pseudonyms change $[PV1,\ldots.,PVC]$ in the graph G, E.

$G([PV_1, \ldots .., PV_C])=\{m|m=\{|[e_1, 1\ldots .e_1, PV_1];$
$[e_2,1\ldots e_2, PV_2];\ldots ..; [ec,1\ldots .ec, PV_c]|\}|$
$ex, ym \Rightarrow ex, yE\}$

So, the probability P of a particular vehicle connected to RS is shown as:

$$P = \Phi(v) \times \sum_{v\in 0\ldots max-zones\_r} \Phi(v) \times \sum_{\substack{Pv=[PV1,\ldots,PVC]) \\ \forall i.Pv_i<aremax\_rdpvt}} \prod_{PV1,\ldots,PVC\in Pv} \times \sum_{g\in G(Pv)} \frac{|p|\, p \in g \wedge \forall_{e\in p} f_{g(e)=1}}{|g|} \quad (5)$$

IV. Conclusion

In this research, we have proposed an advanced method to improve user privacy in terms of dynamic pseudonyms, while focusing on multiple mix-zones over road networks. Our technique is based on multiple mix-zones using advanced cryptographic communication schemes to protect user privacy against various attacks, where number of pseudonym search user requests are limited in given timeframe. After having a detailed analysis of available literature, we observed that existing schemes only deal with the methods that comprise of a single pseudonym change. However, an attacker can easily trace a single pseudonym change during any basic communication under mix-zone schemes. In this paper, we have gradually encouraged each vehicle to change their pseudonym dynamically by using (DPMM) approach inside and outside mix-zone. We have further proposed a new reputation based dynamic pseudonym change protocol for location privacy protection.

On the basis of detailed analysis of results, it has been inferred that our simulation results have outperformed existing techniques such as EPCS (Efficient Pseudonym Changing Schemes for Location Privacy Protection), RPCLP (Reputation-based Pseudonym Change for Location Privacy in Vehicular Networks) and MODP (Mix-zones optimal deployment for protecting location privacy). Furthermore, we obtained better results in terms of achieving high privacy protection rate with a smaller number of pseudonym changes. In our future work, we will examine vehicle to vehicle communication privacy along with focusing on user behavior inside and outside mix-zones over road networks.

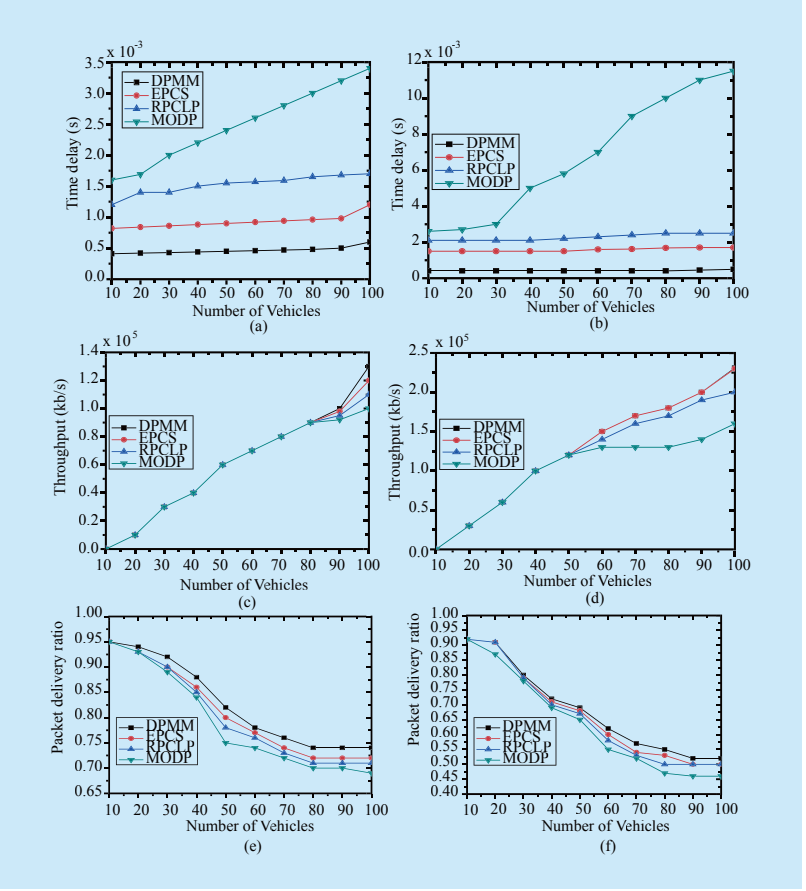

Fig. 5 *Performace Evaluation*

Acknowledgment

This paper has been supported by the National Natural Science Foundation of China (Grant No. 61401040，Grant No. 61372110).

References

[1] Imran Memon (2015). Authentication User's Privacy: An Integrating Location Privacy Protection Algorithm for Secure Moving Objects in Location Based Services. Wireless Personal Communications Volume 82, Issue 3 , pp 1585-1600.

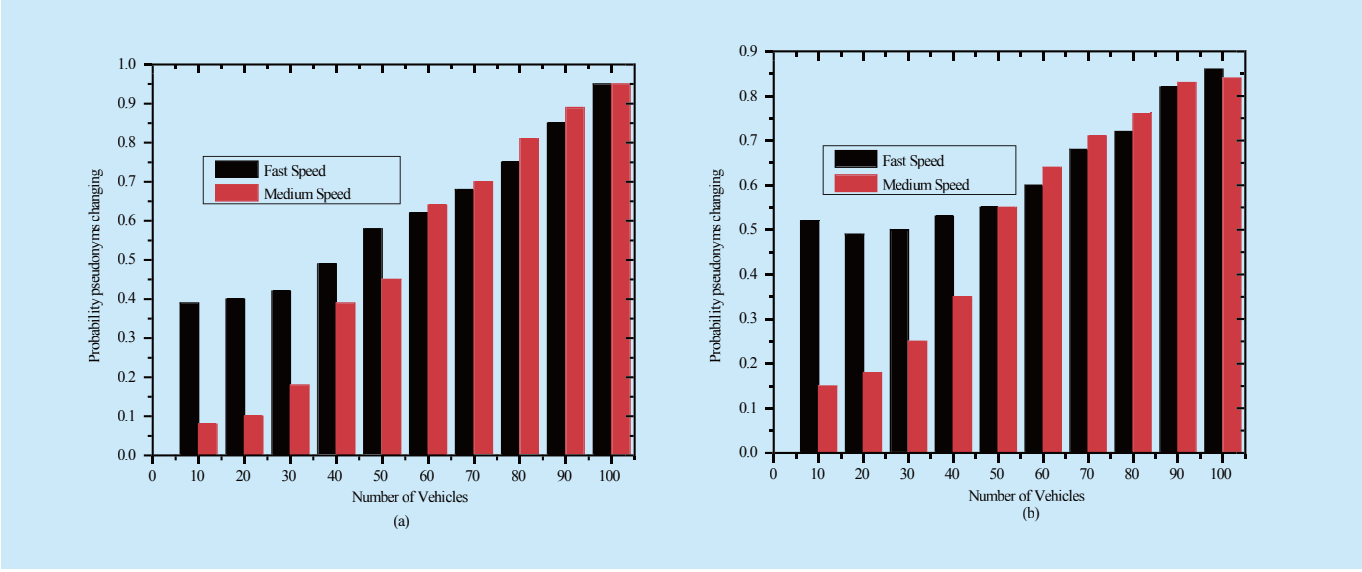

Fig. 6 *Probability pseudonyms changing in various speed*

[2] Imran Memon(2015). A Secure and Efficient Communication Scheme with Authenticated Key Establishment Protocol for Road Networks. Wireless Personal Communications Volume 85, Issue 3 , pp 1167-1191

[3] Imran Memon, Ling Chen, Abdul Majid , Mingqi Lv, Ibrar Hussain, Gencai Chen(2015).Travel Recommendation Using Geo-tagged Photos in Social Media for Tourist. Wireless Personal Communications Volume 80, Issue 4 , pp 1347-1362.

[4] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy," Proc. - IEEE INFOCOM, pp. 972–980, 2012.

[5] K. Moghraoui, "An Efficient Pseudonym Change Protocol Based on Trusted Neighbours for Privacy and Anonymity in VANETs," pp. 93–99.

[6] Yuanyuan Pan, Jianqing Li. Cooperative pseudonym change scheme based on the number of neighbors in VANETs. Journal of Network and Computer Applications 36 (2013):1599–1609.

[7] Song Guo, Deze Zeng, Yang Xiang. Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications. Parallel and Distributed Systems, IEEE Transactions on, Issue Date: Nov. 2014.

[8] Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri.Protocol of Change Pseudonyms for VANETs. 9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks, Local Computer Networks Workshops (LCN Workshops), 2013 IEEE 38th Conference on. pp. 162–7, ISBN: 978-1-4799-0539-3, 21–24 October 2013, Sydney, NSW

[9] J. Freudiger, M. H. Manshaei, J.-Y. L. Boudec, and J.-P. Hubaux, "On the age of pseudonyms in mobile ad hoc networks," INFOCOM, 2010 Proceedings IEEE, pp. 1–9, Mar. 2010.

[10] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," IEEE Vehicular Networking Conference, pp. 1–8, Oct. 2009.

[11] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. S. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," Vehicular Technology, IEEE Transactions on, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[12] Imran Memon, Qasim Ali Arain(2016).Dynamic path privacy protection framework for continuous query service over road networks.World Wide Web.pp 1–33.doi:10.1007/s11280-016-0403-3

[13] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mixzones for location privacy in vehicular networks," ACM Win-ITS, 2007.

[14] J. Freudiger, H.Manshaei, et.al, "On non-cooperative location privacy: a game-theoretic analysis," In: Proceedings of the ACM Conference on Computer and Communications Security(CCS), Chicago: ACM, pp. 324-337, 2009

[15] 10. Shiode, N., Li, C., Batty, M., Longley, P., & Maguire, D. (2002). The impact and penetration of location-based services. CASA Working Paper 50. http://www.casa.ucl.ac.uk/working_papers/paper50.pdf (accessed June 23, 2010).

[16] . Virrantaus, K., Markkula, J., Garmash, A., Terziyan, V., Veijalainen, J., Katanosov, A. et al. (2001). Developing GIS-supported location-based services. In Proc. of the international conference on Web information systems engineering (Vol. 2, pp. 66–75)

[17] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. "Silent cascade: enhancing location privacy without communication QoS degradation," In Proceedings of SPC, pp. 165–180, 2006.
[18] B. Palanisamy and L. Liu. "MobiMix: protecting location privacy with mix zones over road networks," Proc. of 27th IEEE International Conference on Data Engineering (ICDE'11), pp.494-505, 2011.
[19] Muhammad Hammad Memon, Jian-Ping Li, Imran Memon, Qasim Ali Arain(2016).GEO matching regions:multiple regions of interests using content based image retrieval based on relative locations.Multimedia Tools and Applications .pp 1–35.doi:10.1007/s11042-016-3834-z
[20] T. Wang and L. Liu. Privacy-Aware Mobile Services over Road Networks In VLDB 2009
[21] J. Meyerowitz and R. Choudhury. Hiding Stars with Fireworks:Location Privacy through Camouflage In MOBICOM 2009
[22] U.S. Census Bureau.TIGER, TIGER/Line and TIGER-related products. Available at http://www.census.gov/geo/www/tiger/
[23] Simulation of urban mobility (SUMO). Available at http://sumo.sourceforge.net
[24] U.S. Geological Survey. http://www.usgs.gov
[25] Yeong-Sheng Chen, Tang-Te Lo, Chiu-Hua Lee, Ai-Chun Pang(2013).Efficient Pseudonym Changing Schemes for Location Privacy Protection in VANETs.2013 International Conference on Connected Vehicles and Expo (ICCVE).DOI 10.1109/ICCVE.2013.185
[26] Bidi Ying, Dimitrios Makraki(2015).Reputation-based Pseudonym Change for Location Privacy in Vehicular Networks.IEEE ICC 2015-Communications software, services and multimedia applicaations symposium.
[27] yipin Sun , Bofeng Zhang, Baokang Zhao, Xiangyu Su, Jinshu Su(2015).Peer-to-Peer Networking and Applications November 2015, Volume 8, Issue 6, pp 1108-1121015).Mix-zones optimal deployment for protecting location privacy in VANET
[28] Shangguang Wang, Tao Lei, Lingyan Zhang, Ching-Hsien Hsu, Fangchun Yang(2016). Offloading mobile data traffic for QoS-aware service provision in vehicular cyber-physical systems Future Gener. Comput. Syst., 61 (2016), pp. 118–127.doi:10.1016/j.future.2015.10.004
[29] S. Wang, C. Fan, C.-H. Hsu, Q. Sun, F(2014). Yang A vertical handoff method via self-selection decision tree for internet of vehicles IEEE Syst. J. (99) (2014), pp. 1–10
[30] Rizwan Akhtar, Supeng Leng, Imran Memon, Mushtaq Ali, Liren Zhang(2015).Architecture of Hybrid Mobile Social Networks for Efficient Content Delivery.Wireless Personal Communications January 2015,Volume 80, Issue 1, pp 85–96
[31] I Aad, JP Hubaux, EW Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", Networking, IEEE/ACM Transactions on Volume 16, August, 2008
[32] Ohta, T., Ogasawara, K., & Kakuda, Y. (2010). End-to-end transfer rate adjustment mechanism for VANET. In 3rd Dependability conference, DEPEND (pp. 1–6), July 18–25, 2010.
[33] Hamieh, A., Ben-Othman, J., & Mokdad, L. (2009). Detection of radio interference attacks in VANET. In IEEE global telecommunications conference, GLOBECOM (pp. 1–5), Nov. 30–Dec. 4, 2009.
[34] Sichitiu, M. L., & Kini, M. (2008). Inter-vehicle communication system: A survey. IEEE Communications Surveys and Tutorials, 10(2), 88–105.
[35] Mishra, T., Garg, D., & Gore, M. M. (2011). A publish/subscribe communication infrastructure for VANET applications. In IEEE advanced information networking and applications (WAINA) workshops (pp. 442–446), March 22–25, 2011.
[36] Soyoung, P., & Cliff, Z. C. (2008). Reliable traffic information propagation in vehicular ad hoc networks. IEEE Sarnoff Symposium Conference (pp. 1–6), April 28–30, 2008.
[37] Muraleedharan, R., & Osadciw, L. A. (2009). Cognitive security protocol for sensor based VANET using swarm intelligence. In 43th IEEE Asilomar signals, systems and computers conference (pp. 288–290), July 1–4
[38] Imran Memon, Ibrar Hussain, Rizwan Akhtar, Gencai Chen(2015).Enhanced Privacy and Authentication:An Efficient and Secure Anonymous Communication for Location Based Service Using Asymmetric Cryptography Scheme. Wireless Personal Communications September 2015, Volume 84, Issue 2, pp 1487–1508
[39] Imran Memon, Mohammed Ramadan Mohammed, Rizwan Akhtar, Hina Memon, Muhammad HammadMemon, Riaz Ahmed Shaikh(2014). Design and Implementation to Authentication over a GSM System Using Certificate-Less Public Key Cryptography (CL-PKC).Wireless Personal Communications November 2014, Volume 79, Issue 1, pp 661–686

Biographies

Qasim Ali Arain, is a Ph.D. candidate at School of Electronic Engineering, Beijing University of Posts and Telecommunication, China. He is currently working as an Assistant Professor in Department of Software Engineering Mehran University of Engineering and Technology, Jamshoro, Pakistan. He has completed his Bachelors in Software Engineering from Mehran UET Jamshoro in 2005 and completed his Masters in Information Technology in 2010.He is a Cisco Certified Academy Instructor (CCAI), Cisco Security Specialist Microsoft

Certified System Engineer (MCSE), Sun Certified Java Programmer SCJP. His current research interest includes Location based services, Network Security and Indoor positioning.

Zhongliang Deng, is a Professor and doctoral supervisor at School of Electronic Engineering, Beijing University of Posts and Telecommunications, China, his current research interests include wireless positioning, GNSS, satellite communications, MEMS and multimedia.

Imran Memon, B.S. Electronics 2008 from IICT University of Sindh Jamshoro, Sindh Pakistan. M.E. Computer Engineering from University of Electronic Science and Technology, Chengdu Sichuan China. He is towards Ph.D. from College of Computer Science and Technology, Zhejiang University. He got Academic Achievement Award 2011–2012 from UESTC China and also got Excellent Performance Award 2011–2012 from UESTC China. He published over 30 research papers in recent years. He serves as an organizing committee chair and TPC member more than 120 international conferences, as well as a reviewer for over 50 international research journals, including IEEE Transactions on Circuits and Systems for Video Technology ,IEEE Transactions on Image Processing, IEEE Transactions on Signal Processing, IEEE Transactions on Multimedia, ,IEEE Multimedia, IEEE Transactions on Industrial Electronics ,IEEE Signal Processing Letters, Journal of Electronic Imaging Information Sciences Computer Vision and Image Understanding, Image and Vision Computing, EURASIP Journal on Advances in Signal Processing ,Computer Standards & Interfaces, Circuits Systems and Signal Processing Journal of Information Science and Engineering, International Journal of Computers and Applications Far East Journal of Experimental and Theoretical Artificial Intelligence, IEE Proc. Vision, Image & Signal Processing, EURASIP Signal Processing IEE Proc. Information Security, Journal of Circuit, System, and Signal Processing, International Journal of Computers and Applications, LNCS Transactions on Data Hiding and Multimedia Security, Signal Processing International Journal of Pattern Recognition and Artificial Intelligence, IEEE Transactions on Information Forensics & Security, IEEE Transactions on Vehicular Technology, Transactions on Internet and Information Systems , Wireless personal communication, Computers & Electrical Engineering , Computer Networks, Wireless networks, Telecommunication systems and others. Current research interests; Artificial intelligence system, Network security, embedded system, Information security, Peer to Peer networks, Location based services, Road network.

Ms. Asma Zubedi, is a Ph.D. candidate at school of Economics and Management, Beijing University of Posts and Telecommunication, China. Her current research interest include Cyber security, ICT, service quality management and Big Data.

Jichao Jiao, is assistant Professor and doctoral supervisor at School of Electronic Engineering, Beijing University of Posts and Telecommunications, China, his current research interests include Indoor positioning, Computer vision and wireless positioning.

Aisha Ashraf, has done B.E. in Computer System from Mehran UET Jamshoro and completed her Masters from the same University; currently she is working as Lab Engineer in Mehran UET Jamshoro.

Muhammad Saad Khan, was born in 1984 in Pakistan. He received his M.Sc Electrical Engineering Degree in 2010 from Blekinge Institute of Technology, Karlskrona, Sweden and BS.c Electrical Engineering Degree in 2007 from Bahauddin Zakariya University Multan, Pakistan. He has been working as a Lecturer in Electrical Engineering Department Bahauddin Zakariya University Pakistan. Currently he is pursuing his PhD Degree at the School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China. His research interests are VLSI design, Microwave and antenna Propagation, RFIC design, Wireless and Optical communications, Low noise amplifiers and Power Amplifiers. Email: saadkhan9@gmail.com