User Privacy Protection Based On Road Network Model for Location Based Services

Qasim Ali Arain, Riaz Ahmed Shaikh, Hina Memon

***Abstract*—To protect the privacy security in LBS service more effectively, extend the Anonymous Server based on traditional LBS system structure, using the fully homomorphic encryption method to ensure the safety of Anonymous Server itself, and designed a LBS privacy protection model, the model uses the onion algorithm and asymmetric encryption methods to protect users' information. The security analysis shows that the model can effectively protect the user identity anonymous, location information and service content in LBS.**

***Keywords*—Location based service, privacy preserving, data encryption, and anonymous communication**

I. INTRODUCTION

Location Based service refers to cooperate through mobile terminals and network to determine the actual location of the mobile user and provides mobile applications with location information's, so can achieve various Services related to the user's Location[1]. The existing LBS service system consists of three parts: basic user terminal, Anonymous Server and LBS Server. However, the existing research is based on the hypothesis that the anonymous device is safe and reliable, and the reliability of the anonymous apparatus at present has not been proved. Second, the LBS awareness data within IoT(Internet of Things) space is very complicated, For example, one user's information may contain identity information, motion trail, behaviors and living habits and so on, compared with the LBS system based on Internet, the LBS system within IoT space is facing more serious privacy issues. To solve above problems, the researchers have put forwarded many relevant solutions [2].

Manuscript Received January 01, 2016; accepted 05th May, 2016; date of current version December 2016

Qasim Ali Arain is with Department of Software Engineering, MUET, Jamshoro, Pakistan (email: qasim_ali_arain@yahoo.com)

Riaz Ahmed Shaikh is with Department of Computer Science, Shah Abdul Latif University, Khairpur, Pakistan (email: riaz.shaikh@salu.edu,2364420763@qq.com)

Hina Memon is with Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan (email: dr.asifkamran@ibt.edu.pk)

Mobile telecommunication is experiencing a tremendous revolution that will change the world. Mobile telecommunication network will be everywhere in such a way that computing will migrate from the traditional desktop towards consumer-oriented computing using smart wireless personal multimedia devices that will communicate with each other. Mobile telecommunication services have been available since the early 1960s and its diffusion was affected by technological innovations such as transition from analogue to digital technology, competition within the industry, spectrum licensing and the harmonization to common technical standards .The system creatively uses Android mobile development technology based on the research of existing products on the market. Android phones have universality, flexible human-machine interaction, multiple network connection mode (GPRS / 3G / WiFi) and powerful data processing capabilities. Making full use of the mobile phone resources in the data acquisition system of agriculture can reduce system costs (such as eliminating the need for the LCD display module of system), which can also provide users with a convenient touch-screen operation and graceful and varied data display mode, settings of system state of itself at any moment, and views of current and historical collected data [3-5].

In addition, the system and fixed agriculture microclimate data acquisition system can also work together in a complementary way to make up for its defects of the expensive way to ensure good coverage for data collection areas. This makes the product much improved and perfected with the improvement in cost, power consumption, operability, system scalability.

[6]Proposed a role-based access Mix-zone privacy security model, its main idea was through the information block storage and encryption authentication to prevent malicious scanning and tracking of location based services. Secure Multi-Marty Population to protect the privacy of IoT environment security. The safe and efficient scheme that uses fuzzy key word to query, the scheme implemented the mien data fuzzy keywords query, while maintaining the confidentiality of the query keywords. Paper proposed a Dissolver system that can realize the cloud data privacy protection and destruction control, the data stored in the Cloud Corner in the form of a cipher text, so that private data won't be attack and leaked in the form of plaintext

 ISSN-2409-6520

throughout its life cycle. [7-8]. Presented a Group of forward agent model to protect the privacy of LBS position, its basic idea was to cut off the correlation between location service request commands and users' identity information [9].

Despite of several great advantages, VANETs also face some challenges in security and privacy. The open essence of wire-less communications and faster mobility of the vehicles in the network puts the security and privacy of the vehicles to a stake. The messages transmitted by the vehicles can be easily eavesdropped by anyone within the network. These messages can then be used by the adversaries to trace the location of the vehicles and the adversaries can easily spy on the people in the network [10-12].Location privacy is one of the major concerns in the field of VANETs. It is basically related to protecting ones real identity and location information. Adversaries should be fended off from recognizing the real identity of the driver and the specific location of that vehicle. One possible solution to provide location privacy to the vehicles in VANETs is the pseudonym scheme [13-17].

II. ROAD NETWORK MESSAGE BROADCASTING SERVICES

Existing LBS system is mostly based on a central server, which is based on Anonymous Server, and the existing research is under the assumption that Anonymous Server itself is reliable; however, there is no authority certificate to prove the reliability of the Anonymous Server. Once the anonymous device is attacked successfully, the user's privacy will get a serious threat. Therefore, extending the Anonymous Server in LBS system and make it safe and reliable is our first-line work [8].

LBS system structure based on extended Anonymous Server as shown in Figure 1, it includes the mobile user terminals, the extended Anonymous Server and a LBS Service Provider. Its process is: users sent its position information, query information and privacy requirements k to the Anonymous Server; Anonymous Server according to the requirements of users' privacy k to extend the user's precise location to be a anonymous area including other k-1 the users; then sent the region and the user's query request to LBS Service Provider, after get the result set, Anonymous Server according to the location of the users to calculate the accurate results meeting the demand of users queries from the result set and then return the query to user. The expanding anonymous device structure includes Anonymous Computing Center, Encryption Center, Knowledge Base, and Query Result Refine Processor.

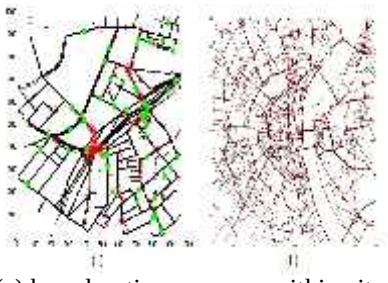

Fig.1 (a) broadcasting message within city area (b) Highway area broadcasting messages

III. ROAD NETWORK MODEL BASED ON USERPRIVACY PROTECTION

After Anonymous Computing Center getting the anonymous area, it will store the anonymous information in the Knowledge Base, and then sent to the LBS server. LBS server include the sender and the receiver, as shown in Figure 2.What Anonymity Server sent to the LBS server are anonymity area and user's service requests, does not contain user's personal information and location information, therefore, transmission between LBS server does not need to use complex data encryption algorithm. Having studied the existing literature and algorithm, the transmission between LBS server is proposed to use the anonymous communication technologies.

Anonymous communication hide the information receiver and the sender's network address, communication relations, identification and other sensitive information in network communications, thus the eavesdropper cannot directly obtain or infer position information, identity information and communication information of both communication sides, thus can realize information sender anonymous, information receiver anonymity, communication relations anonymous between entities, location anonymous(inability to identify the location of the information sender and the receiver, mobile information, route information and topology information), etc., so as to realize the data transmission and the safety of the classified data communication privacy protection.

a.Vehicle terminal function module

Vehicle terminal APP chooses ecplise4.3 as development environment and SQLite as database to storage and read data from the terminal. The main implement of road network for LBSs exchanging the information packaged and verified in accordance with the protocol with the data collection terminal via Bluetooth ; uploading the data via GRPS; storing data in SQLite databases; displaying data.

b. Data exchange

Establishing communication between vehicles and data collection terminal modules via Bluetooth .The specific procedure is to acquire the local Bluetooth device, find the remote device, pair and connect. After that, you can perform data communication and processing. Data processing mainly refers to the analysis, extraction and repacking for the accepted "parameter frame" collected from terminal

 ISSN-2409-6520

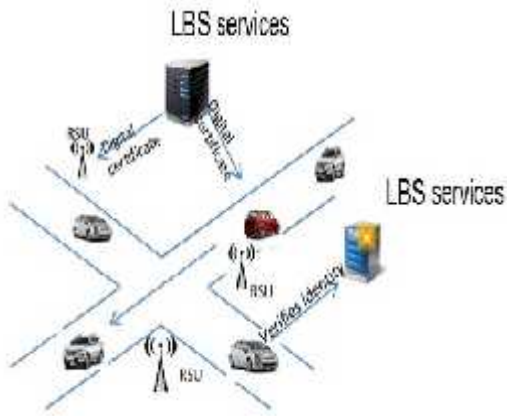

Figure.2: Road network User Privacy Protection Model

The existing anonymous communication algorithm mainly includes the MIX, Onion Routing algorithm flooding algorithm etc. The Onion Routing algorithm is used to pay attention to the real-time data communication and the effectiveness and practicability of the anonymous system, this conformed the requirement of LBS server communication, therefore, this model based on the algorithm to realize the communication of sensory data and location information. Onion routing is based on the channel to realize the data message transmission, so we need multiple nodes to establish channel, subsequent data transmitted through the channel in turn. The LBS privacy protection model using Onion Routing algorithm needs three phases: establish a channel, packet generation and transfer, release the channel. LBS security model are shown in Figure 3 below.

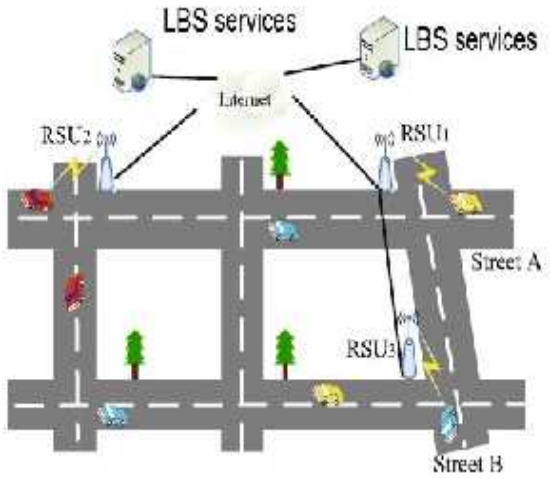

Figure.3: LBS privacy security model

1) The establishment of the communication channel: the establishment of channel needs at least three nodes. Assume that there are four nodes A, B, C, D. With B and C as intermediate proxy node need to use the anonymous agent, node A sends the message, node D receives the message. Nodes A, D according to the routing information get the information of next communication nodes, thus creating a self-anonymous communication link. Each intermediate node is responsible for the asymmetric encryption and decryption of the message Q and encrypts anonymous communication nodes by the private key.

2) Packet generation and transmission: the first packet needs to establish a secure communication channel and the subsequent packets just need to along the channel to transmit, the last packet need to release the channel. Before sending, packets need to get the next jump through node's public key PK. For example, node A sends a packet Q to node B. well first, using the public key PB generate by node B to encrypt Q into Q ' at the same time save the PB; then sending Q' to B, after receiving Q', B will use its own public key SB to decode Q'into Q, and then continue to use the public key PC generate by node C to encrypt Q and then sent to C, and so on. Node A keeps a counter k to record the number of packets.

3) Release the communication channel: When counter k to the last packet, node A will send out the last packet at the same time reset k=0 and delete the PB. Also, after send the last packet, node B and C will delete the private key it has kept.

Communication processes between different nodes is shown in Figure 4 below.

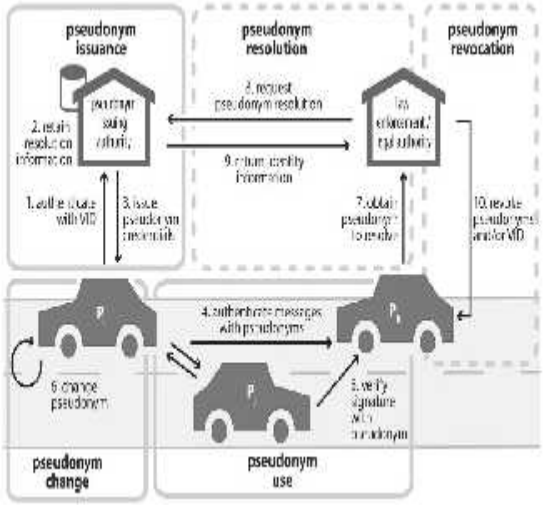

Figure.4: Encryption process of the anonymous communications

According to Figure 3 and Figure 4 we can know, using anonymous communication mechanism between LBS servers, asymmetric encryption mechanism between different nodes data transmission, dual mechanism insure the security of user's information between LBS servers transmission. As a result, after expanded anonymous server and LBS security model the service request arrive service provider, thus ensure the user's information will not be tampered or leak.

IV. MATHEMATICAL MODEL

a. Equation of state for position targeting

The section headings are in boldface capital and lowercase letters. Second level headings are typed as part of the succeeding paragraph (like the subsection heading of this paragraph). In transfer alignment, because the master inertial navigation system precision than the sub inertial navigation system is several orders of magnitude higher, the master INS is as a reference, the calculated navigation coordinate system can be

ISSN-2409-6520

considered true navigation coordinate system. Navigation coordinate n is regarded as the East - North - Up geography coordinate system. n' Represents the SINS navigation coordinate calculation. Represents the inertial coordinate system, represents the carrier coordinates. The error state equation is derived as follows:

First velocity error equations.

Inertial navigation basic equation, $\dot{V}^n = f^n - 2(\mu_{ie} + \mu_{en}) \times V^n + g^n$ (1)

In the formula, μ_{ie} is the earth rotation angular velocity, μ_{en} is navigation system angular velocity relative to the earth. f^n Is a projection of the accelerometer output is in the navigation system. V^n Is navigation system of the line speed? g^n Is a projection of acceleration of gravity in the navigation system?

By using the variation method, we calculate the formula,

$\delta\dot{V}^n = \delta f^n - 2(\delta\mu_{ie} + \delta\mu_{en}) \times V^n - 2(\mu_{ie} + \mu_{en}) \times \delta V^n + \delta g^n$ (2)

¨ n

Stands for the sub inertial navigation computing platform misalignment angles. $f^{n'}$ Is the actual accelerometer output. The projection of accelerometer measurement error in navigation system is ∇^n, δg^n =0(As the chariot moves on the ground, the errors can be ignored). Formula of (3) is brought into the formula of (2). We get the formula of (4).

$\delta f^n = f^{n'} - f^n$ (3)

$\delta\dot{V}^n = f^n \times \ddot{}^n - 2(\delta\mu_{ie} + \delta\mu_{en}) \times V^n - 2(\mu_{ie} + \mu_{en}) \times \delta V^n + \nabla^n$ (4)

Then the attitude error equation. The attitude calculation matrix of sub inertial navigation is $C_b^{n'}$, the attitude calculation matrix of main inertial navigation is C_b^n. Their relationships are as follows.

$C_b^{n'} = C_n^{n'} C_b^n$ (5)

In the formula (5), $C_n^{n'}$ is a mathematical strap down platform alignment error. In the small misalignment angles case, $C_n^{n'}$ can be expressed as formula (6)

$$C_n^{n'} = I - \ddot{}^n \times = \begin{bmatrix} 1 & \ddot{}_z & -\ddot{}_y \\ -\ddot{}_z & 1 & \ddot{}_x \\ \ddot{}_y & -\ddot{}_x & 1 \end{bmatrix} \quad (6)$$

¨ ¨ ¨

In the formula (6), $_x$, $_y$, $_z$ respectively stand as three misalignment angles in directions of north, east, up.

$\mu_{in'}^{n'} = C_n^{n'} \mu_{in}^n + \ddot{}^n = \mu_{in}^n - \ddot{}^n \times \mu_{in}^n + \ddot{}^n$ (7)

We write a formula $\delta\mu_{in}^n = \delta\mu_{ie}^n + \delta\mu_{en}^n$, $£^n$ is the equivalent gyro drift in the navigation system. After simplification, omitting the two order terms, we get the attitude error formula (8).

$\ddot{}^n = -\mu_{in}^n \times \ddot{}^n + \delta\mu_{in}^n - £^n$ (8)

Here is device error equation.

The main error of gyro and accelerometer can be divided into constant error and random walk error. We set the symbols as follows, $£_d$ is gyro constant error, $£_w$ is gyro random walk error, ∇_d is the constant error of accelerometer, ∇_w and is random walk error of accelerometer. w_∇, $w_£$ represent different standard deviation of white noise. The accelerometer and gyro error equations are as follows.

$\dot{\nabla} = \dot{\nabla}_d + \dot{\nabla}_w = w_\nabla$ (9)

$£ = £_d + £_w = w_£$ (10)

Integrating the above error equation, we get the state equations of transfer alignment.

$\dot{X} = FX + W$ (11)

Due to the chariot as the research object, in the establishment of the state equation, we think that the vertical channel speed is always zero; we don't consider the effect of vertical channel. L Stands for the geographic latitude, where is the carrier in. ^{a} represents the longitude. h Represents the height R_e stands for the earth radius 6378245m e represents the earth elasticity 1/298.3. $R_E = R_e/(1 - e\sin^2 L)$ this represents the local prime vertical plane curvature radius. $R_N = R_e/(1 + 2e - 3e\sin^2 L)$, this indicates that the main curvature radius, it with the prime plane vertical. $C_b^n = (T_{ij})_{3\times3}$, Each part of equation of state are as follows:

$X = \left[\delta V_x^n \quad \delta V_y^n \quad \ddot{}_x^n \quad \ddot{}_y^n \quad \ddot{}_z^n \quad \nabla_x \quad \nabla_y \quad £_x \quad £_y \quad £_z\right]^T$ (12)

$$F = \begin{bmatrix} \frac{V_y \tan L}{(R_E+h)} & 2\omega_{ie}\sin L + \frac{V_x \tan L}{(R_E+h)} & 0 & -f_z^n & f_y^n & T_{11} & T_{12} & 0 & 0 & 0 \\ -2\left(\omega_{ie}\sin L + \frac{V_x \tan L}{(R_E+h)}\right) & 0 & f_z^n & 0 & -f_x^n & T_{21} & T_{22} & 0 & 0 & 0 \\ 0 & \frac{1}{(R_N+h)} & 0 & \left(\omega_{ie}\sin L + \frac{V_x \tan L}{R_E+h}\right) & -\left(\omega_{ie}\cos L + \frac{V_x}{R_E+h}\right) & 0 & 0 & T_{11} & T_{12} & T_{13} \\ \frac{1}{(R_E+h)} & 0 & -\left(\omega_{ie}\sin L + \frac{V_x \tan L}{R_E+h}\right) & 0 & \frac{V_y}{R_N+h} & 0 & 0 & T_{21} & T_{22} & T_{23} \\ \frac{\tan L}{(R_E+h)} & 0 & \left(\omega_{ie}\cos L + \frac{V_x}{R_E+h}\right) & \frac{V_y}{R_N+h} & 0 & 0 & 0 & T_{31} & T_{32} & T_{33} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (13)$$

$W = \left[w_{vx} \quad w_{vy} \quad w_{\ddot{}x} \quad w_{\ddot{}y} \quad w_{\ddot{}z} \quad w_{\nabla x} \quad w_{\nabla y} \quad w_{£x} \quad w_{£y} \quad w_{£z}\right]^T$ (14)

In *W*, during the simulation, each element can be regarded as zero mean white noise.

a. The measurement equation of transfer alignment:

δV_x^n, δV_y^n represent the main, sub ins level speed difference, $\delta¥$, $\delta¯$, $\delta\cdot$ represent the roll angle, pitch angle and yaw angle difference. Transfer alignment measurement equation as follows:

$Z = HX + V$ (15)

ISSN-2409-6520

In the formula, we use the measured element representation formula.

$$Z = \begin{bmatrix} ¢V_x^n & ¢V_y^n & ¢¥ & ¢^{-} & ¢\cdot \end{bmatrix}^T \quad (16)$$

The observation matrix

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{-T_{22}}{\sqrt{1-T_{32}^2}} & \frac{T_{12}}{\sqrt{1-T_{32}^2}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{T_{21}T_{33}-T_{31}T_{23}}{T_{31}^2+T_{33}^2} & \frac{T_{13}T_{31}-T_{11}T_{33}}{T_{31}^2+T_{33}^2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{T_{12}T_{32}}{T_{12}^2+T_{22}^2} & \frac{-T_{22}T_{32}}{T_{12}^2+T_{22}^2} & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (17)$$

The observation noise,

$$V = [V_{vx} \quad V_{vy} \quad V_{\cdot\cdot x} \quad V_{\cdot\cdot y} \quad V_{\cdot\cdot z}]^T \quad (18)$$

During the simulation, each element can be regarded as zero mean white noise.

b. Calman filtering algorithm:

We use the method of discretization to process the state equation and measurement equation.

$$X_k = \Phi_{k,k-1} X_{k-1} + \Gamma_{k-1} W_{k-1} \quad (19)$$

$$Z_k = H_k X_k + V_k \quad (20)$$

In the above formula, X_k represents the system state vector, $\Phi_{k,k-1}$ represents the system transfer matrix, Γ_{k-1} represents the system noise matrix, W_{k-1} represents a discrete system white noise with zero mean, Z_k is a measurement vector, H_k is a measurement matrix, V_k is a discrete zero mean white measurement noise vector. X_k, W_{k-1}, V_k they are not related.

Put the following basic equation to represent the discretization Calman filter.

The state estimation equation of prediction is as follows.

$$\hat{X}_{k/k-1} = \Phi_{k,k-1} \hat{X}_{k-1} \quad (21)$$

Variance prediction equation is as follows.

$$P_{k/k\text{-}1} = \Phi_{k,k\text{-}1} P_{k\text{-}1} \Phi_{k,k-1}^T + \Gamma_{k-1} Q_{k-1} \Gamma_{k-1}^T \quad (22)$$

State estimate update equation is as follows.

$$\hat{X}_k = \hat{X}_{k/k-1} + K_k (Z_k - H_k \hat{X}_{k/k-1}) \quad (23)$$

Variance iterative update equation is as follows.

$$P_k = (I - K_k H_k) P_{k/k-1} (I - K_k H_k)^T + K_k R_k K_k^T \quad (24)$$

The filter gain renewal equation is as follows.

$$K_k = P_{k/k-1} H_k^T (H_k P_{k/k-1} H_k^T + R_k)^{-1} \quad (25)$$

V. SECURITY ANALYSIS

Based on conventional LBS system, the LBS privacy protection model based on extended anonymous server expanded the structure of Anonymous Server, at the same time built a privacy protection model that can support real identity, physical location and service content.

After receiving the service request Q, the Anonymous Server encrypt the request first, and then store the encrypted information in Knowledge Base, and after Anonymous Server receives the query result set from LBS server, refining the result set. then the Refine Processor will send an authentication to the Knowledge Base, only this authentication is effective, the Knowledge Base decrypt Q' with its private key SK and send it to Refine Processor to screen correct results. Therefore, the requests information, including user's location information and status information are effectively protection in Anonymous Server, thus avoiding leaking users' information because of Anonymous Server be attacked.

In LBS server's internal, we use Onion Routing algorithm, the package information use each forwarding node's public key to encrypt and decrypting turn until the request data arrive the target client, any communication nodes does not know the true identity information of message sender and the receiver, thus can guarantee the security of both identity information and location privacy, and also ensure the security of location information, identity information and other data in transmission and storage phase.

By extending the Anonymous Server and LBS server double safeguard, the user's identity, location information and service content have been effectively protected during the service request process, so as to avoid its privacy leak.

VI. CONCLUSION

Analyzing the problems of existing LBS service framework, using encryption algorithm extends the traditional Anonymous Server to ensure its own security, at the same time, using anonymous communication to design LBS privacy protection model based on expanded Anonymous Server, this model can effectively protect the safety of users' privacy in LBS service. The next step in the research work is mainly prototype design and implementation of the privacy security model, and to verify the effectiveness and practicability of the model through the experiment, at the same time, to expand the model to the more complex Internet of Things environment and make it has a wider range of application.

REFERENCES

[1] Lu, R., Lin, X., Luan, T. H., Liang, X., & Shen, X, 2012, Pseudonym changing at social spots: An effective strategy for location privacy in VANETs. IEEE Transactions on Vehicular Technology, 61(1), 86–96.

[2] Fuentes, J. M. D., González-Tablas, A. I., Ribagorda, A, 2010, Overview of security issues in vehicular ad-hoc networks. In Handbook of research on mobility and computing. http://www.igi-global.com

[3] Samara, G., Al-Salihy, W. A. H., Sures, R, 2010, Security analysis of vehicular ad hoc networks. In Second international conference on network applications, protocols and services IEEE, pp. 55–60.

[4] Parno, B., & Perrig, A, 2005, Challenges in securing vehicular networks. In Proceedings of HotNets -IV.

[5] Caliskan, M., Graupner, D., Mauve, M, 2006, Decentralized discovery of free parking places. In Proceedings of the Third ACM International

 ISSN-2409-6520

Workshop on Vehicular Ad Hoc Networks (VANET 2006, Los Angeles, CA, USA, pp.30–39.

[6] Raya, M., & Hubaux, J. P, 2005, The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN '05), Alexandria, Va,USA, pp. 11–21.

[7] Gerlach, M., Festag, A., Leinmuller, T., Goldacker, G., Harsch, C, 2007, Security architecture for vehicular communication fourth international workshop on intelligent transportation (WIT2007).

[8] Calandriello, G., Papadimitratos, P., Hubaux, J.-P., Lioy, A, 2007, Efficient and robust pseudonymous authentication in VANET. In Proceedings of the ACM international workshop on vehicular ad hoc networks (VANET),p. 19–28.

[9] Raya, M., & Hubaux, J.P, 2005, The security of vehicular ad hoc networks. In SASN '05: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks ,New York, NY, USA: ACM, p. 11–21.

[10] Rass, S., Fuchs, S., Schaffer,M.,Kyamakya,K., 2008, Howto protect privacy in floating car data systems. In VANET'08: Proceedings of the fifth ACM international workshop on vehicular inter-networking,New York, NY, USA: ACM, pp.17–22.

[11] Chaurasia, B.K., Verma, S., 2008, Maximizing anonymity of a vehicle through pseudonym updation. In WICON '08: Proceedings of the 4th annual international conference on wireless internet. Brussels, Belgium; ICST (Institute for Com- puter Sciences, Social-Informatics and Telecommunications Engineering); p. 1–6.

[12] Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., Sezaki, K., 2005, Caravan: Providing location privacy for VANET. In Embedded security in cars (ESCAR).

[13] Gerlach,M., Festag, A., Leinmuller, T., Goldacker, G., Harsch C., 2007, Security architecture for vehicular communication. In fourth international workshop on intelligent transportation (WIT2007).

[14] Li, M., Sampigethaya, K., Huang, L., Poovendran, R., 2006, Swing & swap: User-centric approaches towards maximizing location privacy. In Proceedings of WPES ,pp. 19–28.

[15] Freudiger, J., Raya, M., Feleghhazi, M., 2007, Mix zones for location privacy in vehicular networks. In Presented at the workshop on wireless networking for intelligent transportation system, Vancouver, BC, Canada, LCA-CONF-2007-016.

[16] Chaum, D, 1982, Blind signatures for untraceable payments. Advances in crypto'82 ,Berlin: Plenum, pp. 199–203.

[17] Lu, R., Lin, X., Zhu, H., Shen, X.,2009, SPARK: A new VANET-based smart parking scheme for large parking lots. In Proceedings of IEEE INFOCOM'09, Rio de Janeiro, Brazil, pp.19–25.

 ISSN-2409-6520