International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Efficient Handoff Based Privacy Preservation for VANET

Sibil Joseph[1], Rajagopal .R[2]

[1]PG Scholar, KCG College of Technology, Department of Electronics and Communication, Chennai, India

[2]Assistant Professor, KCG College of Technology, Department of Electronics and Communication, Chennai, India

Abstract: ***VANET is a technology which make use of moving vehicles having location based senses to make a communication network for communicating between vehicle and the base station to transfer safety and non-safety related data like traffic alert, navigation, accident and multimedia applications and so on. Vanet having mainly three parameter they are vehicle, roadside unit and regional trusted authority. Roadside unit is the base station for particular region and regional trusted authority which act as a server. The security in privacy preservation and handoff between the base stations i.e. road side unit between different technologies is a serious issue in VANET. In the proposed system we are providing Elliptic Curve Diffie Hellman (ECDH) cryptography using public key where we have different key for encryption and decryption and we make use of digital signature for data integrity for security, the authorized authority have the access to track the vehicle using regional trusted authority server which have all information of the vehicle which make sense of non-repudiation in VANET and efficient vertical handoff between Road Side Unit based on signal strength and bandwidth between WLAN and WiMAX insure efficient coverage and multimedia access to the vehicle.***

Keywords: Elliptic Curve Diffie Hellman, Road Side Unit, Reginal Trusted Authority, Vertical Handoff

1. Introduction

Wireless networks is providing mobility and unprecedented freedom for wireless devises. VANET is a wireless network from the subnetwork of MANET. There are two type of wireless network they are infrastructure and Ad hoc Networks. Infrastructure network is having fixed base station and base station connected to the network using wired interface. Ad hoc Networks network is non-infrastructure network which make use of wireless interface to connect base station and the user network. There are three type of Ad hoc Networks network they are wireless mesh network (WMN), wireless sensor network (WSN), mobile ad-hoc network (MANET). A wireless mesh network (WMN) is a network made of mesh tropology consists of radio nodes mesh router, mesh gateway and clients. A wireless sensor network (WSN) consists sensor network which is used to monitor environmental and non-environmental conditions like temperature, sound, pressure, motion, humidity, pollution and so on. These sensor network will frequently transform information with maser station and work adequately the help of centralized monitoring system. A mobile ad-hoc network is a network which connected by wireless links which having is self-configuring capability and is infrastructure less network. In MANET each user can join and leave the network without any permission at any time and each user is free to move anywhere in network coverage area.

VANET is part of MANET which make use of moving vehicle to make a mobile network to communicate between vehicle and base station i.e. the roadside unit. VANET composes of three main component they are Vehicle, Road Side Unit (RSU) act as base station and the Regional Trusted Authority (RTA). To provide an efficient communication and coverage to vehicle we need to have interoperation between different wireless networks. Each vehicle in the VANET network is connected to a particular network, if we consider only one wireless network to be accessed to base station i.e. is the RSU then network will not be efficient when that particular access technology is not available but some other wireless network is available. So here we are proposing a system for VANET which can interoperate with various WLAN and WiMAX, this is done using vertical-handoff between the networks. Meanwhile there are different Security Vulnerabilities for VANET like jamming, forgery, privacy, authentication, false position indication and so on, because of this data which is communicating in the network should be protected so we are using an Elliptical Curve Diffie Hellman (ECDH) for data communication.

2. Related Works

VANET provides various research in communication between vehicles to make a safety related application like accident avidness, traffic jam, criminal identification, vehicle tracing and so on. VANET implementation using ID based Cryptography [6,3,4,13} which provide privacy preservation and non-repudiation to VANET using public key cryptography here it use user defined ID for communication, which intern secure privet data of the vehicle and the authorized authority can get all the information of the vehicle like tracing of vehicle so it provide non-repudiation concept. communication between vehicle to vehicle and vehicle to Road Side Unit (RSU) is done using ID based online offline cryptography because vehicle to vehicle communication should be always active i.e. it should transfer real time data to vehicle and RSU to vehicle is done using ID based cryptography (IBS), where ones the vehicle is registered on RSU it can make offline communication between RSU and vehicle without any authentication. When analyzing on cryptography for VANET [1, 14, 22, 17] it show that asymmetric key cryptography is highly secure than symmetric key cryptography where symmetric key cryptography is faster than asymmetric key cryptography

because key length is less. In the proposed system we are using Elliptic Curve Diffie Hellman (ECDH) cryptography which is an asymmetric key cryptography which is highly secure. Routing protocol for identifying whether serves provider is available if not it will use internet for accessing vehicle communication [8, 10, 17, 20, 16]. VANET is mainly having three main block [5, 16] they are vehicle, Road Side Unit [RSU] and Reginal Trusted Authority [RTA]. Vehicle which communicate to each other which transfer real time information [16,24], RSU which is a base station which cover certain area and transfer safety and multimedia message [6,16,9] , RTA [2,20] which is a server which is having all information about vehicle and RSU which help for tracing of vehicle for authorized people. From all this works it do not show any information about Handoff between different Road Side Unit (RSU) or base station, there are different access technology's like Wi-Fi, WiMAX, UMTS, and various WLAN so it essential for a hand off between RSU for getting access to this technology. Using vertical handoff we are make handoff between different access technologies' [18, 19]. In this proposed system we are providing an efficient handoff for base station i.e. RSU between WLAN and WiMAX using vertical handoff based on signal strength and QOS which make a vast coverage and multimedia application for VANET.

3. System Implementation

The VANET network is implements using mainly three components as shown in Figure-1. Vehicle which is the user is registered in Regional Trusted Authority [RTA] when entering VANET environment. Vehicle have its own user defined ID which preserve private data and is registered with RTA. We are using Elliptic Curve Diffie Hellman (ECDH) Public Key Cryptography algorithms, where it have different key for encryption and decryption. Using Public Key Cryptography (PKC) each vehicle create its own private and public key and it is known to RTA. RTA pass the public key of the vehicles to RSU and it transfer to vehicles in network using this public key vehicle make communication. ECDH make high security by adding digital signature.

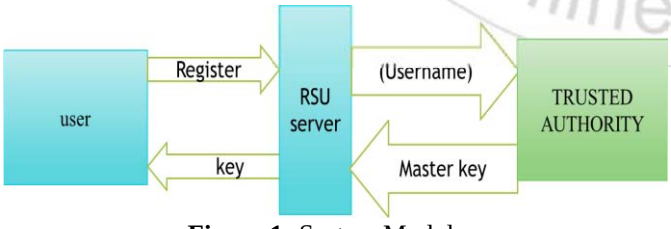

Figure 1: System Modules

In the existing system we Road Side Unit (RSU) which is the base station using UMTS and it cannot interoperate with other mobile technology's this is a disadvantages for the existing VANET technologies. So here we are proposing a vertical handover scheme for VANET to use WiMAX and WLAN as shown in Figure-2.

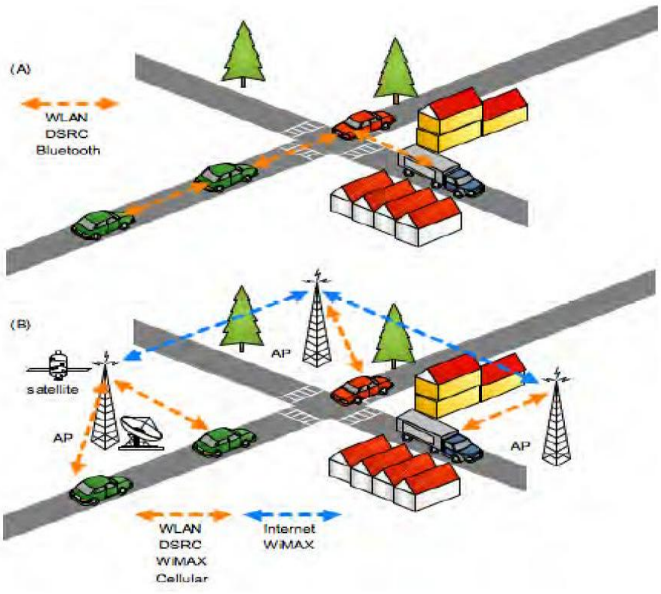

Figure 2: Handoff Architecture

VANET is having mainly two types of applications they are safety related and non-safety related application. Safety related message is the road information such as vehicle collision alert, emergency warning of stopped vehicle, and warning about road condition and so on. Non safety related application is for Internet connectivity related message and application such as web browsing, entertainment and mobile commerce. Internet is essential for internet and multimedia related application, so handoff scheme between different access technologies is essential in VANET because there will be absence of signal availability i.e. non coverage area for a particular access technology so interoperation between different access technologies for base station or RSU is critical one. Hand off between same networks is done using horizontal handoff and different technology is done using vertical handoff. Vertical Handoff process consist of three main phases they are network discovery, handoff decision and triggering and handoff execution

Network discovery: mobile terminal should know which all wireless network are available and accessible.

Handoff decision and triggering: using vertical handoff algorithm it provide handoff request between base station i.e. RSU based on network parameter like connection time, bandwidth, power, cost, security level, ,QOS and user preferences.

Handoff execution: This is the phase where Actual transfer of the current base station to the new base station and data transfer session take place through new RSU.

4. Cryptographic Method

The proposed system efficient handoff based privacy preservation for VANET is based on public key cryptography using Elliptic Curve Diffie Hellman (ECDH). This provide a highly efficient privacy preservation for

VANET by preserving privet information of the vehicle. The system use user defined ID which do not have any information about the real identification of the vehicle. We are having public and privet key, using public key the message is encrypted and sent to the receiving user or vehicle and at the receiver end it is decrypted using the privet key of the receiver this show the basic public key cryptography. The Elliptic Curve Diffie Hellman (ECDH) operation is illustrated in Figure-3.

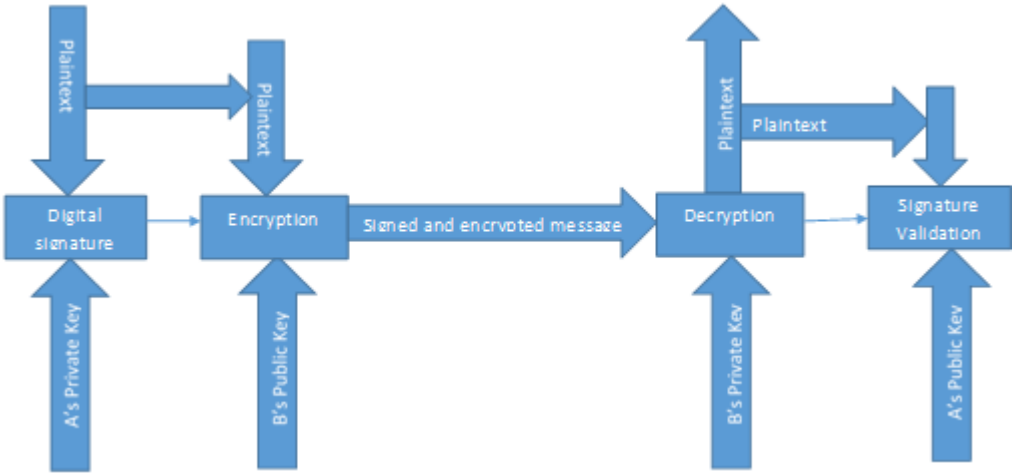

Figure 3: Cryptographic Process

From the figure we have two user i.e. user A and B, to make sure privacy preservation and security to the user using ECDH we have digital signature and encryption of message. User A make digital signature using private key of A and encrypt the message to B using public key of B then it is transmitted in a secure channel and it is received by the user B, B receive the encrypted and signed message and it decrypt the message using privet key of user B and verify the signature using public key of A. This make a efficient privacy in VANET.

5. Handoff Algorithm

Handoff is essential for handoff in VANET between various access technologies, here we are providing a handoff between WLAN and WiMAX which is initiated using certain parameters like signal strength, Signal-to-Noise Ratio (SNR) and Bandwidth. From the flow diagram in Figure-4 show the illustration of Handoff.

First we consider user or vehicle is in the coverage of WLAN, if the SNR is above some threshold and having good coverage then the user or vehicle will be in coverage of WALN, it also check the number of connection in the current WLAN and if the we have less number of connection then there will be only small delay and the connection is efficient. If SNR is below the threshold and user is having low coverage mobile node will scan for WWAN i.e. here we are using WiMAX and it will initiate a vertical handoff between WLAN and WiMAX. Vertical handoff is also initiated even though we are having a good coverage at the present base station if number of user connected to the present base station or RSU is more so that delay in overall connection will be more so it initiate Vertical handoff between the both. When switching of WLAN to WWAN the WWAN will always scan the WLAN for better coverage and bandwidth for hand off and the process will continue. We have added the connection parameter which make efficient QOS to the entire system which make a new handoff system for VANET.

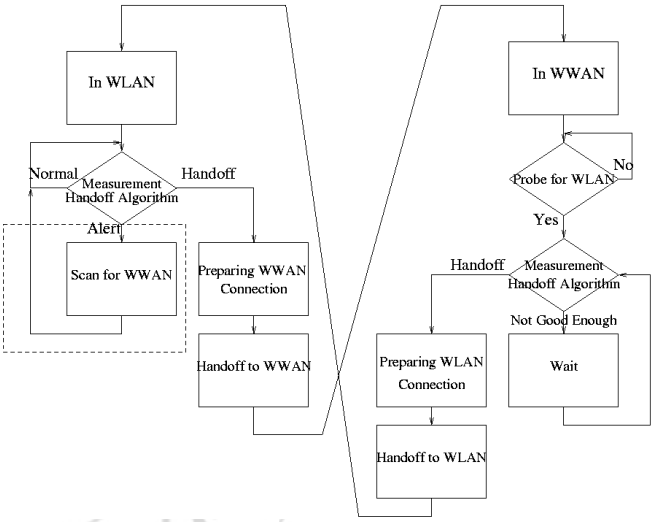

Figure 4: Handoff Algorithm

6. Program Modules

The program modules of the proposed system is of four parts they are

1. Network selection
2. Fading Detection
3. Vertical Handoff between WiMAX/WLAN
4. Effective handoff

6.1 Network Selection

The proposed system is having basically three component they are the user or the vehicle, Road side unit (RSU) or base station and the Reginal Trusted Authority (RTA). In this project we use two type RSU access point i.e. WLAN and WiMAX.

The network selection module should know information of access point that are available at the location, so that it can select one among them according to their priority. WiMAX

system is having three type of network component they are the base station (BS), Relay station and user. In the system implementation we implement three type of relay station as follows

1) Standardized fixed relays station: this relay station is the fixed position which relay information to user
2) femto or picocell base station which is having wireless capability to relay information in a wireless medium, using this function it can relay the fixed femto or picocell BSs with wireless relay functionalities it can relay information to user and WLAN and WiMAX station.
3) Mobile relays station: which is used to relay in formation to user any SS with relaying functionality.

6.2 Fading Detection

This module is used to detect fading of access signal. Fading of signal is due to movement of the mobile node or the user i.e. it will move away from the coverage area of the access point. If the user is stationary always there will not be any signal fading.

Fading is measured by using some threshold if the user is under some threshold value it require a handoff to new access point which have a good coverage for the user, if the user having signal strength above the threshold it do not require any hand off because it satisfy all the requirement to stay in the correct location. Due to fading system experience delay in data transition so it is essential to avoid this fading. In the proposed system fading occur when the mobile node move away from access point.

6.3 Vertical Handoff

Vertical handoff is used when we need to interact with different access technology's .If the mobile node and the base station detect fading of signal handoff is initiated. Handoff between same networks is done using horizontal handoff method. In our system we are proposing vertical handoff i.e. we are providing a efficient handoff implementation between WiMAX and WLAN both are of different access technology. WiMAX is having IEEE standard of IEEE 802.16 and a bandwidth of 2.5GHz. WLAN have IEEE standard of IEEE 802.11 and a bandwidth of 2.4 GHz.

6.4 Effective Handoff

The proposed system implementation handoff is based on two parameter the signal fading and number of user attached to the RSU or base station.

In the normal handoff the handoff is made if the user node detect a signal fading, in this system we are including the number of user attachment in the given access point, i.e. if more number of users are attached to the current base station conjugation will occur and it result in delay in packet delivery. So in this system handoff will be initiated even though we do not have a fading signal but if the number of user connect to the base station is more than the users will switch to nearby base station to form a hand off, this will make a handoff and we will have good QOS and network quality.

7. Results

Stimulation the proposed system is done using network stimulator (ns2) using a Nam window and Xgraph. Nam window is used to show the stimulation output and Xgraph is used to trace the graph. System output include creating the VANET environment, Attack by malicious node, Vertical handoff and security enhancement using the proposed system. We have Creating VANET Environment using 14 mobile user i.e. the vehicle, three WLAN base station and one WiMAX base station. Using WLAN and WiMAX it create a handoff between the both according to signal fading based on threshold and number of user connected. In the result part we have crated malicious effected part and the proposed system to detect and overcome the malicious base station using Elliptic Curve Diffie Hellman (ECDH) cryptography. We create a WLAN node as malicious node so that all the packed which are transmitted through that specific base station or the RSU are dropped and it effect the entire communication system. Using the proposed system it can easily detect the malicious base station and indicate the user that the particular base station is malicious node and system avoid the communication through that node and preserve the privacy and enhance the security using ECDH cryptography. We analyzed the entire system using Xgraph by three parameter Throughput, Packet delay and overhead.

Throughput show the amount of information that is delivered at a particular time. Analyzing the graph Figure-5 it show that the throughput for current proposed system offers higher throughput than the existing VANET systems. The proposed system avoid and detect the malicious node so that it avoid the path through that node, so we are having a good throughput.

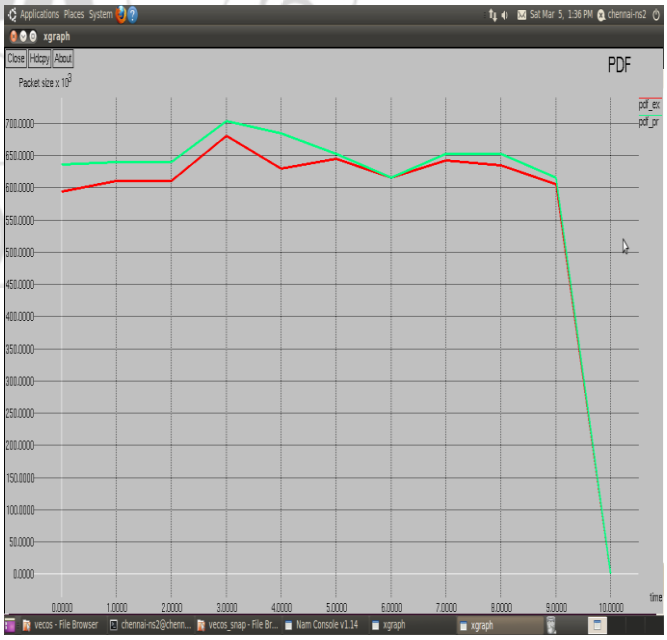

Figure 5: Throughput

Packet delay is the delay occur in transmitting packet form source to destination. Analyzing the packet delay graph shown in Figure-6 the, it shows that we are having low delay rate because we have the capability of detection and

avoidance of malicious node and it increase the data transfer rate and avoid data flow infinity.

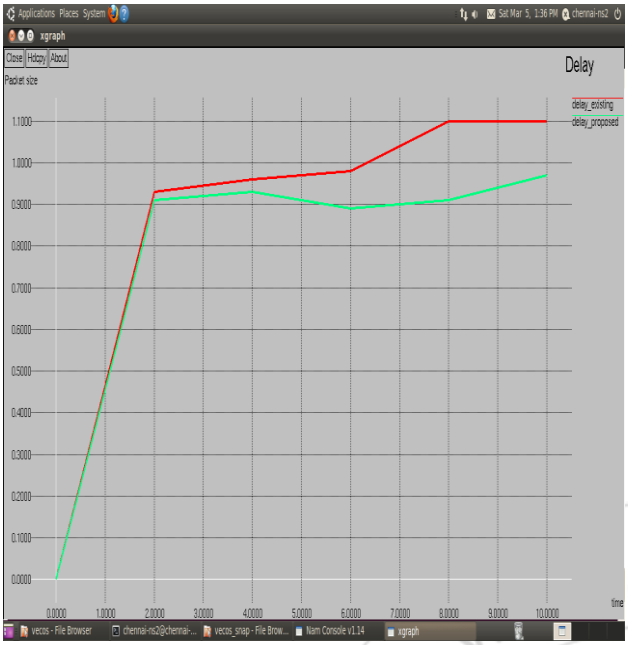

Figure 6: Delay

Packet overhead is the computation and time complexity in the system. From the graph Figure-7 show overhand graph which show high overhead because we are using a efficient handoff using Elliptic Curve Diffie Hellman (ECDH) cryptography which provide enough security and avoid malicious node, so it is having a complex computation and time consuming this result in a bit high overhead than the system which do not have a secure communication system.

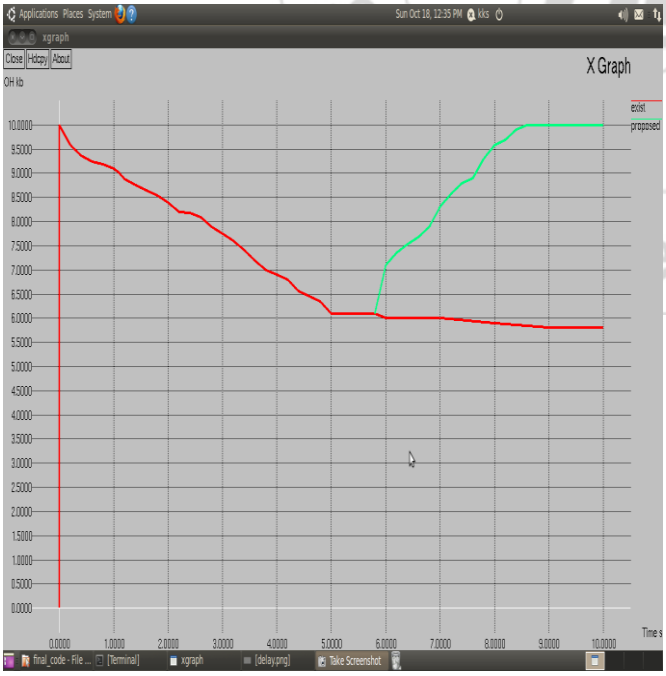

Figure 7: Overhead

8. Conclusion

The proposed system efficient handoff based privacy-preservation for VANETS provide efficient handoff between WLAN and WiMAX and make a large coverage and multimedia application to the vehicle. High security and location preservation of vehicle is done using Elliptic Curve Diffie Hellman (ECDH) cryptography. Analysis and performance show that the proposed system is efficient and adequate for VANET environment. The security in privacy and preservation can be farther enhanced using a hybrid cryptography combining asymmetric and symmetric key cryptography. The proposed VANET system analyses the efficient handoff between WLAN and WiMAX and it can be extended to all the current access technology available so that VANT can have vast coverage over the globe.

References

[1] Anjali Patil, and Rajeshwari Goudar, "A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices" International Journal of scientific & technology research volume 2, issue 8, August.2013.

[2] Daojing He, Sammy Chan, Mohsen Guizani, Haomiao Yang, and Boyang Zhou, "Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks" IEEE Transactions on Parallel and Distributed Systems, VOL. 26, NO. 4, April.2015.

[3] H. Dok et al, "Privacy Issues of Vehicular Ad-Hoc Networks," Int'l J. Future Generation Comm. and Networking, vol. 3, no. 1, pp. 17-32.

[4] H. Lu, J. Li, and M. Guizani "A Novel ID-Based Authentication Framework with Adaptive Privacy Preservation for VANETs," Proc. Comm. and Applications Conf. (ComComAp), pp. 345-350, March.2012.

[5] Huang Lu, Jie Li, and Guizani "A novel ID-based authentication framework with adaptive privacy preservation for VANETs" International Journal on Communication and Application (345 – 350), volume 23-No .31, June.2012.

[6] Jie Li, Senior Member, IEEE, Huang Lu, Member, IEEE, and Mohsen Guizani, Fellow, IEEE "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs" Ieee Transactions On Parallel And Distributed Systems, VOL. 26, NO. 4, APRIL 2015.

[7] Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks" IEEE Transactions On Vehicular Technology, Vol. 60, No. 1 August.2011.

[8] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey" IEEE Communication Surveys & Tutorials, VOL. 17, NO. 1, First Quarter 2015.

[9] J. Sun et al, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, February.2010.

[10] Khaleel Mershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks" IEEE Transactions on Vehicular Technology, VOL. 62, NO. 2, February. 2013.

[11] Lo-Yao Yeh and Yu-Cheng Lin, "A Proxy-Based Authentication and Billing Scheme With Incentive-Aware Multihop Forwarding for Vehicular Networks" IEEE Transactions On Intelligent Transportation Systems, Vol. 15, No. 4, May.2014.
[12] M. Alimohammadi, and A. A. Pouyan (2014) "Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET" International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February.2014.
[13] Mansoor Ebrahim, Shujaat Khan, and Umer Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis" International Journal of Computer Applications (0975 – 8887), Volume 61– No.20, January.2013.
[14] Mina Rahbari1 and Mohammad Ali Jabreil Jamali, "Efficient Detection Of Sybil Attack Based On Cryptography In VANET" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, April.2011.
[15] Shanmuga Priya.S , and Erana Veerappa Dinesh.S, "A Novel Approach for Data Acquisition and Handover Scheme in VANET" Shanmuga Priya.S et al, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5.
[16] Sibil Joseph, Rajagopal. R "Enhanced Privacy Preservation and Non-Repudiation for VANET's" International Journal for Research in Emerging Science and Technology, VOLUME-3, ISSUE-2, FEB-2016.
[17] Song Guo, Senior Member, IEEE, Deze Zeng, Member, IEEE, and Yang Xiang, Senior Member, IEEE, "Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications" IEEE Transactions on Parallel And Distributed Systems, Vol. 25, No. 11, December.2014.
[18] SuKyoung Lee, Member, IEEE, Kotikalapudi Sriram, Fellow, IEEE, Kyungsoo Kim, Yoon Hyuk Kim, and Nada Golmie, Member, IEEE, "Vertical Handoff Decision Algorithms for Providing Optimized Performance in Heterogeneous Wireless Networks" IEEE Transactions On Vehicular Technology, Vol. 58, No. 2, March.2009.
[19] Tarik Taleb, Senior Member, IEEE, and Adlen Ksentini, Senior Member, IEEE "VECOS: A Vehicular Connection Steering Protocol" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 64, NO. 3, MARCH 2015.
[20] Xiaodong Lin, Xiaoting Sun, Xiaoyu Wang, Chenxi Zhang, Pin-Han Ho, and Xuemin Shen, "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving" IEEE Transactions On Wireless Communications, VOL. 7, NO. 12, December.2008.
[21] Xiaoyan Zhu, Shunrong Jiang,and Hui Li, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks" IEEE Transactions on Vehicular Technology, vol.63, no. 2, February.2014.
[22] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang, "Securing Mobile Ad Hoc Networks with Certificate less Public Keys" IEEE Transactions On Dependable and Secure Computing, VOL. 3, NO. 4, December.2006.
[23] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin (Sherman) Shen, and Jinshu Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications" IEEE Transactions on Vehicular Technology, vol. 23, no. 4, February.2010.