International Journal of Engineering & Technology, 7 (4.10) (2018) 832-836

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Multivariate Quadratic Quasigroup Polynomial based Cryptosystem in Vanet

K. Selvakumar[1]*, S. Naveen Kumar[2]

[1]*Department of Information Technology, Annamalai University.*
[2]*Department of Computer Science and Engineering, Annamalai University.*
**Corresponding author E-mail: kskaucse@gmail.com*

Abstract

Vehicular Ad-hoc Network (VANET) is a developing transmission system to abet in the everyday organization of vehicular traffic and safety of vehicles (nodes). Unsigned verification is one of the key necessities in VANET gives the confidentiality of the root of the message. Current security conventions in VANET's gives unsigned verification depends on the two-tier architecture, comprises of two VANET components, particularly nodes and Roadside Units (RsU's) functioning as the key developing server (KDS). This protocol depends densely on RsU's to give unsigned identification to the nodes. In this paper, we propose the K-means Cluster Head algorithm which is utilized for guide assortment, for both personal-best ('p_{best}') and global-best ('g_{best}'), are observed a tremendously successful and complete well evaluate to the before existing methods. Here, we also propose an asymmetric encryption algorithm, with emphasis on Multivariate Quadratic Quasigroups (MVQQ) algorithm, in a circumstance of VANET. We set forward prime pseudonyms reasonably make a long time cycle that are worn to interact with semi-confided in experts and alternate pseudonyms with a minor lifetime which are utilized to talk with different nodes.

Keywords: *K-means Cluster Head Algorithm, Multivariate Quadratic Quasigroup (MVQQ), Pseudonym Authentication, VANET (Vehicular Ad-Hoc Network).*

1. Introduction

Vehicles associated with each other's throughout an ad-hoc pattern to design a wireless framework called "Vehicular Ad-Hoc Network". A VANET is sprouting innovations builds a mobile framework by through impactful vehicles as nodes. In VANET, communications are reassigned among nodes and additionally Roadside Units (RsU's). It continues as both server and customer. VANET is an advancement that incorporates the backbone of recent age remote systems to the vehicles. VANET manufacture a full-bodied ad-hoc arrangement which is surrounded by mobile nodes and roadside units as explained in [1]. Making inter communication between the node to avoid accident and journey comfort and safely. From out of network by using sensor vehicles can communicate to the destination. In a radio communication band, at least multi nodes or an Intelligent Transportation System (ITS) stations may consequently interface, making an Ad-Hoc network, which implies that all stations known the position, speed, and direction of alternate stations, getting to be proficient for giving alternate data. It also develops the essential segments of the architecture, to be specific: Onboard Unit (ObU), Roadside Unit (RsU) and the WAVE (Wireless Access in Vehicular Environment) interface. The principle motivation behind a VANET is to furnish highway travelers with security [2]. The peculiarity of a VANET is the foundation of a protected association in a brief timeframe, given the high portability of the nodes. In this investigation, we utilize an asymmetric encryption algorithm, especially a Multivariate Quadratic Quasigroup (MVQQ). It also provides other effects such as authenticating user, producing and distribute certificates, maintain, managing and revoke certificates. Open Key Infrastructure (OKI) is an infrastructure in which various impacts occur and isn't a route or algorithm itself, so OKI comprises various perspectives to enable the infrastructure to work. And additionally authentication, OKI in like manner engages the use of giving reliability, non-repudiation and encryption. In this paper, we set forward a hierarchical pseudonymous-based protocol that confirms a node for the time of the communication with different nodes in network and gives contingent anonymity. In this way, except if a node includes an improper (malicious) confusion, it is difficult to pursue the node. Be that as it may, on the off chance that a cruel movement is recognized, the offender is followed and accordingly revoked from the network. The expiry purpose of pseudonyms is to be balanced by the infrequent/heavily RsU's distribution. Our work is the expanded form of exertion [6] and it covers best in class in regards to pseudonymous verification issues and more point by point examination with extensive mock-up results.

2. Interconnected Work

Security in VANET'S are generally contemplated for some researchers, yet the greater part of them may not be presented the data about execution or assessment of symmetric or asymmetric algorithms functioning in a genuine situation of the vehicular network. Consequently, in our insight, this paper shows the value examination since it demonstrates the execution period of MVQQ algorithm in different scenarios of VANET. [3] The objective is to accomplish nearby security by utilizing locally available radar and to recognize acquaintance also affirm the declared GPS organizes. They utilized the present area which is depending on cells (through which we accomplish nearby security) that makes a

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

communication network. Here we catalogue these analyst efforts in the pseudonymous-based authentication. Many of the pseudonymous platform plans are put into operation with the assistance of OKI. These methods utilize OKI dependent certificates which are emotionally involved with comparable private keys. [4] Circulate more number of pseudonyms amongst nodes which analogous private keys. The scheme presupposes an inescapable utilization of RsU's that add to the framework load and along these lines, the general daily practice of the framework moves forward. The Certificate Distribution Authority (CDA) issues the initial pseudonym allowing maintaining the organization between the initial pseudonyms and the actual identification of the node. Nonetheless, the original uniqueness in CDA's database are encrypted by other article is called as Revocation Distribution Authority (RDA) and accordingly, CDA is incapable to decrypt these original identification. Alternate pseudonyms are delivered by RsU upon a fruitful authentication of the initial pseudonym. A node at that point televises the communication signed with the connected private key of the alternate pseudonym and the recipient node confirms the messages with a related open key arranged in the alternate pseudonym [5], [7]. After analyzing the article, we deduct the progressive restrictions; pseudonymous-based courses of action bring about the powerful computational, communicational and capacity because of the presence of CRL (Certificate Revocation List) [8]. Here, we analyzed asymmetric algorithm (MVQQ algorithm) into genuine. [9] The authors affirm that the effective organization of vehicular transmission expects the Vehicle-to-Vehicle (V-V) and Vehicle-to-Infrastructure (V-I) transmission with security to road-side safety and road-side traffic. Moreover, the three primary cryptography designs were researched as open key, symmetric key, and personality based cryptography, which is utilized for the security of the system. [10] Suggested another clustering model for powerful transmission among the VANET and to build it alongside the security algorithms so that the transmission among the VANET nodes can be made more increasingly proficient way. In VANET the information and quantitative assessment of this algorithm offers the low-overhead, data integrity, authentication and privacy, and real-time constraints.

3. K-means Cluster Head Algorithm

In this paper, we propose the K-means Cluster Head algorithm to partitioning the nodes into *k* clustering. Particularly the parameter *k* is known to be difficult to pick the best nodes among a wide range of nodes.

K-means clustering aims to division n perceptions into *k* clusters in which every perception belongs to the cluster with the nearby mean, serving as a prototype of the cluster. Cluster analysis groups the figures objects subject to data found in information that depicts the items and their endeavors. In this paper, we propose K-means clustering [11], mainly aims to demonstrate the connection between the nodes to conveys which is best using both Personal-best ('p_{best}') and global-best ('g_{best}'), are observed to be highly efficient and implemented all around contrasted with the as of now displayed techniques [12].

Personal-best (p_{best}): The individual finest location identified to the molecule *i* is the perfect detect that the molecule has visited (past estimation of x_i), yielding the best wellness worth for that molecule. For a minimization assignment, a circumstance yielding the littler capacity worth is viewed as have wellness. The symbol f(X) utilized to mean the target utility that is being limited. The revise equation is

$$p_{best\,id}^{(t+1)} = \{X_{id}^{(t)} \; if \; f(X_{id}^{(t+1)}) \geq f\left(p_{best\,id}^{(t)}\right)$$

$$p_{best\,id}^{(t+1)} = \{X_{id}^{(t+1)} \; if \; f(X_{id}^{(t+1)}) < f(p_{best\,id}^{(t)})$$

Global-best (g_{best}): The g_{best} provides a quicker rate of the union at the cost of power. This g_{best} manages a distinct finest arrangement known the global-best speck, over the fully molecule in the group. In the end, every one of the molecules will converge to this position, so on the off chance that it isn't simplified frequently, the flock may meet prematurely.

4. Security in VANET

Late investigations display to use asymmetric encryption in the embedded systems, as it is insisted by Ref [13], who assessed the asymmetric encryption algorithms with more security levels, RSA's with a key-size to 3076 bits and ECC's with a key-size to 512 bits in the embedded systems.

4.1. Asymmetric Algorithm

Multivariate Quadratic Quasigroup (MVQQ)

The encryption algorithms beforehand presented the security subject to computationally separated numerical issues: Computational viability of the discrete logarithm count and integer factoring. Another plan of open key was made, known as Multivariate Quadric Quasigroups (MVQQ). In Ref [14], this algorithm depends on the Quadratic Multivariate polynomials and Quasigroups changes, holds the accompanying characteristics i.e.

Step 1: This is an out-quantum algorithm;

Step 2: In the encryption methodology, the speed is similar to another open key encryption processes subject to Multivariate Quadrics;

Step 3: In the decryption, the speed counterparts to a commonplace encryption of a symmetric block;

Step 4: Exceedingly parallelizes, dissimilar to different algorithms which are fundamentally progressive.

The conventional detail of the MVQQ design is a common Multivariate Quadric system.

$$A \circ B \circ C: \{0, 1\}^n \rightarrow \{0, 1\}^n$$

Where A and C are multi non-singular linear transformations, B´ is a bijective multivariate quadratic aligning over $\{0, 1\}^n$. The encryption algorithm with an open key is the immediate procedure for the use of n multivariate polynomials

$B = \{B_i(s_1 \ldots\ldots s_n) \mid i = 1, \ldots, n\}$ Over the vector s = (s_1……..s_n), in other words, r = B(s).

What can be represented as,

$$r = B(s) \equiv y \equiv DZ$$

As shown by Ref [13] tests performed in equipment exhibit that MVQQ consists of an average symmetric block encryption. In Ref. [15], investigations with a framework of sensors, launch that MVQQ is couple of sizes quicker than the algorithms like RSA's and ECC's. This reality certified that the outcomes gained in Ref [14] while using programming; he contemplated that the digital signature made by MVQQ is 300 to 70000 times quicker than RSA's and ECC's digital signature. In any case, the dominance of MVQQ can accomplish 10.000 times. In addition, as shown by Ref [16], that the MVQQ algorithm gives another way for the cryptography field; in general it develops new encryption systems of open key, and in addition upgrading the existing ones. Ref [17], [18]. They have utilizes these three principles by connection: The preparing time, storage and processor utilization. The outcomes demonstrated that MVQQ is a decent algorithm for embedded systems since it is superior to ECC's and RSA's.

Generating an open and private key for the MVQQ algorithm:

Input: Integer *r*, where *r*=5*l* and *l*>28.

Output: Open key **O**: *r* Multivariate Quadratic Polynomials O_i $(y_1,\ldots\ldots,y_n)$, i=1,……,n,
Private Key: Two nonsingular Boolean matrices S and U of order r * r and eight Quasigroups $*_1\ldots,*_8$

1. Create two nonsingular r * r Boolean matrices S and U (uniformly at random).
2. Call the method for definition of $O^{'}(r) : \{0,1\}^r \rightarrow \{0,1\}^r$ and from there also obtain the Quasigroups $*_1,\ldots,*_8$.
3. Figure x=S($O^{'}$($U(y)$)) where y=($y_1,\ldots..,y_n$)
4. Output - The Open key is x as r Multivariate Quadratic polynomials $O_i(y_1,\ldots y_n)$, i=1,….n, and the private key is the tuple $(S,U,*_1,\ldots.,*_8)$.

5. Proposed Pseudonymous Authentication

Table 1: Notations

Notations	Explanations
V_i	Initiator/ Sender vehicle
V_R	Receiver vehicle
VID_i	Initiator's/ Sender's vehicle ID
$IK_i, AK_i, IK'_i, AK'_i, IK''_i, AK''_i$	MVQQ open/ private key pairs of V_i
IK_{CDA}, AK_{CDA}	MVQQ open/ private key pairs of CDA
IK_{CAP}	Paillier open key pair of CDA
IK_{RsU}/ AK_{RsU}	MVQQ open/ private key pair of RsU
T_{CDA}, T_{CDA}'	Expiration time of initial pseudonym set by CDA
T_{RsU}	Expiration time of alternate pseudonym set by RsU

5.1. Vehicular certification and initial pseudonym formation

At the time, sender/initiator node (V_i) develops an arbitrary number k (This irregular worth is next encrypted in CDA's Paillier open key) and a open/private MVQQ's key pair

IK_i/AK_i.

V_i sends this data alongside the VID_i to CDA.

Step 1: $V_i \rightarrow$ CDA: $k||IK_i||VID_i$.

The V_i deliver this data to the CDA by means of some safe channel (for instance node visits the CDA). Step1 is mandatory only once.
CDA approves the VID_i. As verifies, it encrypts VID_i with single open key developed by RDA, encrypts k with its Paillier open key IK_{CAP}, produces a termination time T_{CDA} and build the successive database (DB) access.
Example of a CDA database:

CDA $\rightarrow$ DB : $(VID_i)_{PK_{RDA}}$ $||T_{CDA}||IK_i||k$

CDA signs $(T_{CDA}||IK_i||(k)_{IK_{CAP}})$, and attach it to V_i as its first initial pseudonym.

Step 2: CDA $\rightarrow V_i$: $(T_{CDA}||IK_i||(k)_{IK_{CAP}})\ AK_{CDA}$

5.2. Restore initial pseudonym

Once the T_{CDA} depart, V_i requirements to get the initial pseudonym again. In such manner, V_i arbitrary preferred a few $k^{'}$, creates a open/private MVQQ key pair

$IK_i^{''}$ / $AK_i^{''}$

Encrypts the information in open key of CDA alongside k and deliver it to CDA by utilizing 3G/4G technology.

Step 3: $V_i \rightarrow$ CDA: $(k||k^{'}||IK_i^{''})\ IK_{CDA}$

In case, the node desire the restore of an initial pseudonym to CDA by means of RsU's then delivered this message to the close-by RsU's that advances this demand to the CDA. On by demand, few unique reason bits in the message utilized that empowers the RsU's to perceive the node is asking for initial pseudonym by means of RsU's or the node is asking the RsU's for a recent alternate pseudonym.

Step 3': $V_i \rightarrow$ RsU $\rightarrow$ CDA: $(k||k^{'}||IK_i^{''})\ IK_{CDA}$

CDA certify this message with perfect k, develop a new termination time $T^{'}_{CDA}$, modernize its database with unique values of $k^{'}$, $IK^{''}_i$ and T_{CDA}. CDA rehashes stage 2, yet encrypts the recently produced the initial pseudonym in $IK^{''}_i$ and delivers return to V_i. In Off the chance that, the demand has originated from RsU's then CDA dispatch this message to V_i by means of RsU's alongside the signed k. The signed number of k generates a company with the advanced value of $k^{'}$. If RsU's advertises this message, V_i analyze it with aged k, prove CDA's signature, decrypt it and transformation its initial pseudonym. Because of encryption, RsU's is helpless to disclose the advanced initial pseudonym to the V_i.

Step 4: CDA $\rightarrow$: V_i $((T_{CDA}||IK_i^{''}||(k^{'})\ IK_{CAP})\ AK_{CDA})\ IK_i^{''}||(k)\ AK_{CDA}$

5.3. Alternate pseudonym formation

RsU's occasionally communicates the messages while declaring the quality. Its additionally consist of the open key of the RsU's. If a node gets this message it demands for the alternate pseudonym. The node creates other open/private MVQQ's key pair ($IK^{'}_i$, $AK^{'}_i$). It encrypts the recently created open key and initial pseudonym, $-k$ and a nonce in RsU's open key and delivers it to the RsU's.

Step 5: $V_i \rightarrow$ RsU $((T_{CDA}||IK_i||(k)\ IK_{CAP})\ AK_{CDA}||IK_i^{''}||-k||\text{nonce})\ IK_{RsU}$.

RsU's check CDA's trademark, encrypts $-k$ with Paillier open key of CDA. RsU's holding the homomorphic addition of one and the other (k) IK_{CAP} and $(-k)$ IK_{CAP}, receives (S) IK_{CAP}.
Where (S) IK_{CAP} = (k) IK_{CAP} + $(-k)$ IK_{CAP}, RsU's deliver the (S) IK_{CAP} to CDA for checking purpose.

Step 6: RsU $\rightarrow$ CDA: (S) IK_{CAP}

CDA decrypts S, catch O (k + ($-k$) = 0) and circulate *verifiable* message to RDA if not deliver *not verifiable.*
Step 7: CDA $\rightarrow$ RsU's: *verifiable* / *not verifiable*.
CDA receives the encrypted value and doesn't serves any idea around that node is utilizing this value. $-k$ is utilized the values to avoid a cruel attack.
Upon earning certification that the message began from V_i, RsU's arrange a alternate pseudonym. It constructs the termination time T_{RsU}, inserts it with recently developed $IK^{'}_i$, and sends it to V_i. The IK'i must be produced by V_i each time an alternate pseudonym is asked. In any case, a node can register again in a lake of MVQQ key pairs.

Step 8: RsU's $\rightarrow V_i$: $((T_{RsU}||IK_i^{'})\ AK_{RsU})\ IK_i^{'}$.

6. Working of a Proposed protocol

In the proposed convention, a client node requires to commune with another user-node using K-means cluster Head and to register with the Certificate Distribution Authority (CDA) in order to get the initial pseudonym through Roadside Unit (RsU). Here, we also provide the encryption and decryption key algorithm is MVQQ. These timeframes is noted as T_{CA} in our convention and locate by CDA at the season of initial pseudonym generation. Coming up next are the wished-for protocols.

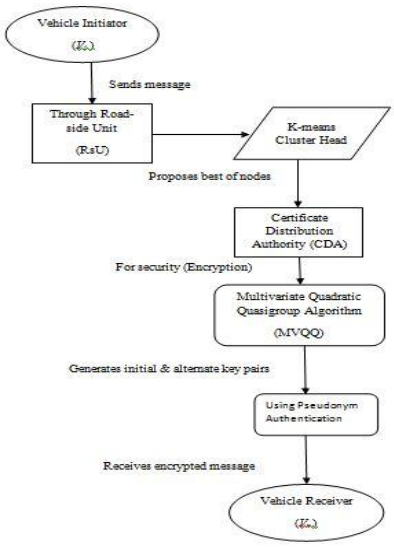


Figure 1: Flow diagram for the recommended protocol

7. Performance Evolution

In this work, we proposed actualized and incorporated algorithm K-means Cluster Head and MVQQ algorithm. At that point information was produced, which enabled us to gauge algorithm execution on a VANET and perusing the outcome next. Here we can see that, in this underlying situation, nodes are found in an area with a separation littler than 100m. Here the nodes are inner the system range and there was no package was disposing of. Utilizing a situation of 10 nodes, where node "0" delivers a communicated message to alternate nodes from the system. In our simulations, this procedure happens on average of 0.4 m. Consequently we feature the productivity of MVQQ, as per what has been tried (tested) by different works already made reference to, however in various contexts of VANET networks. With MVQQ algorithm, the perfect key size is 160 bits comparing with the others, in this way, obviously, it is seen in Figure. 4 a developing curve if the amount of information movements in the VANET increments. Here we assess the execution of our proposed protocol in significant viewpoints. The viewpoints are going to be assessing the execution of RsU's if the node significantly asking the RsU's for alternate pseudonym by giving an initial pseudonym. If RsU's checks the initial pseudonym essentially includes the demand and afterward produces and deliver the alternate pseudonym to the node. Hence, the RsU's can essentially check whether it is capable to implement this task on a persistent condition to the nodes.

Packet Delivery Ratio (PDR)

PDR is characterized as total number of packets effectively deposited to the total sent packets. PDR describe as the number of packets is sent from origin to terminal if the proportion of the network is expanded in any strategy that implies by utilizing this procedure network assistance improves. The formula for PDR is:

PDR = (RCV/SND)*100

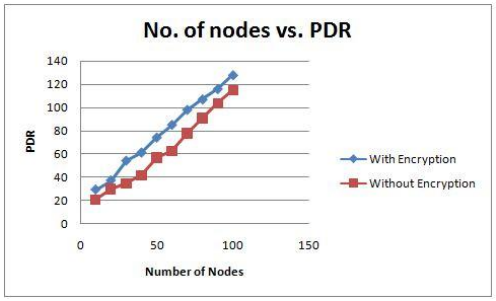


Figure 2: Packet Delivery Ratio w.r.t speed between the nodes.Throughput

Throughput is a part of how many units of information a system may processed in the given time. Throughput characterizes as the measure of information come truly from a station to another station. Bits are exchanged from starting with one place then onto another place in every second. On the off chance that the throughput is high then data transfer capacity. Usage is better beneath us notice the formula of throughput as:

Throughput = bitspersecond

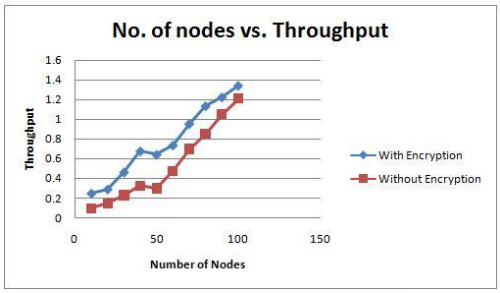


Figure 3: Throughput w.r.t speed between the nodes.*End-End Delay*

It is imperative to find the bang of encryption overhead on the end-end delay with expanding measure of nodes and speeds.

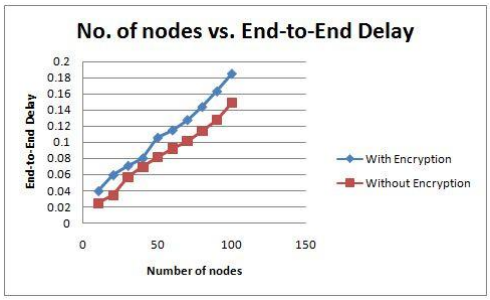


Figure 4: End-End Delay w.r.t speed between the nodes.*Packet over Head*

The time it proceeds to broadcast the information on a packet-switched framework. Every packet needs additional bytes of format data which is stored in the packet header, when mixed with the assembly and disassembly of packets, decreases the overall transmission speed of the crude information. Here the graph shows a packet over head diagram between the current and proposed approach. The proposed methodology is longer in the overhead protocol than the base methodology.

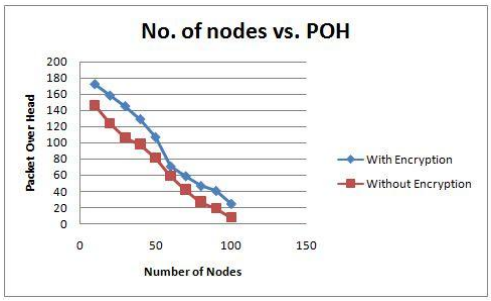


Figure 5: Packet Over Head w.r.t speed between the nodes.

8. Conclusion

The main parts of this paper include an indication of VANETs and K-means Cluster Head. The current research challenges of VANETs are focused on security. VANET carry numerous security concerns. The security investigation of our proposed convention exhibits the elasticity against different security warnings. In this paper, we proposed the MVQQ algorithm for security purposes. Moreover, the execution assessment of our proposed convention not just displays the computational and correspondence overhead.

Here, we minimize the delay and maximize the sanctuary and appropriate performance. In this paper, we also propose an effective Pseudonym Authentication protocol alongside upgrading security.

References

[1] Pathan, Al-Sakib Khan , "Security of Self- Organizing Networks: MANET, WSN, WMN, VANET", CRC press, 2011.

[2] Sumra, I.A., H.B. Hasbullah, J. Manan and A. Lail, 2011, "Comparative study of security hardware modules (EDR, TPD and TPM) in VANET", at king Saud University Riyadh.

[3] Choudhary, G.K., 2007. Providing VANET security through position verification. MSc., Thesis, Old Dominion University.

[4] M. Raya and J. Hubaux, ''the security of vehicular ad hoc networks'', in Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw., 2005, pp. 11–21.

[5] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy, "Efficient and robust pseudonymous authentication in VANET", *In VANET '07*, New York, NY, USA, September 2007. ACM, pages 19–28.

[6] U. Rajput,F. Abbas, H. Eun, R. Hussain, and H. Oh, ''A two level privacy preserving pseudonymous authentication protocol for VANET'', in Proc.IEEE Int.Conf. Wireless Mobile Comput., Netw. Commun. (WiMob), Oct. 2015, pp. 643–650.

[7] J. Petit, F. Schaub, M. Feiri, and F. Kargl, ''Pseudonym schemes in vehicular networks: A survey'', IEEE Commun. Surveys Tut., vol. 17, no. 1, 2015, 1st Quart., pp. 228–255.

[8] Studer, A.; Shi, E.; Fan Bai; Perrig, A, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs", *Sensor, Mesh and Ad Hoc Communications and Networks, SECON '09. 6th Annual IEEE Communications Society Conference on*, vol., no., June 2009, pp.1-9, 22-26.

[9] Rajni, M.K. and P. Singh, 2013. An encryption algorithm to evaluate performance of V2V communication in vanet. Int. J. Cryptography Inform. Security.

[10] Bhuvaneshwari, S., G. Divya, K.B. Kirithika and S. Nithya, 2014. A novel approach for secured data transmission in VANET through clustering. J. Electron. Commun. Eng., 9: 23-30.

[11] Nasrin Taherkhani and Samuel Pierre, "Centralized and Localized Data Congestion Control Strategy for Vehicular Ad Hoc Networks Using a Machine Learning Clustering Algorithm", Senior Member, IEEE transactions on Intelligent Transport Systems, Vol. 17, No. 11, November 2016.

[12] Nikhil Padhye, Juergen Branke and Sanaz Mostaghim, "Empirical Comparison of MOPSO Methods - Guide Selection and Diversity Preservation", 2009.

[13] Tanwar, G., G. Singh and V. Gaur, 2010. Secured encryption-concept and challenge. Int. J. Comput. Applic., 2: 89-94.

[14] Gligoroski, D., S. Markovski and S. Knapskog, 2008. "A public key block cipher based on multivariate quadratic quasigroups" in Cornell University Library.

[15] Maia, R.J.M., P.S.L.M. Barreto and B.T. Oliveira, 2010. Implementation of multivariate quadratic quasigroup for wireless sensor network. Trans. Comput. Sci. XI, 6480: 64-78. DOI: 10.1007/978-3-642- 17697-5_4.

[16] Ahlawat, R., K. Gupta and S.K. Pal, 2009. From MQ to MQQ cryptography: Weaknesses and new solutions. Universia Holding.

[17] Quirino, G. and E. Moreno, 2013a. Architectural evaluation of asymmetric algorithms in ARM processors. Int. J. Electron. Electrical Eng., 1: 39-43. DOI: 10.12720/ijeee.1.1.39-43.

[18] Quirino, G. and E. Moreno, 2013b. Architectural evaluation of algorithms RSA, ECC and MQQ in ARM processors. Int. J. Comput. Netw. Commun., 5: 153-168. DOI: 10.5121/ijcnc.2013.5212.