A New Novel Approach for Secured Encryption Concept and Challenges with MVQQ in VANET

K. Selvakumar, S. Naveen Kumar, Shaji. K. A. Theodore

Abstract: ***VANET is the most growing research area in wireless communications, In VANET each vehicle can act as a node and can give correspondence among nodes and road-side base stations with a point of offering for capable and secure transport. In VANET the vehicle looks like an intelligent mobile node which is outfitted for communicating with its neighbors and distinctive vehicles within the network. This network also provides the Intelligence Transportation System (ITS) for users, ensuring operation is moving to be in a simple manner. In this paper, we propose an asymmetric encryption algorithm with emphasis on Multivariate Quadratic Quasigroups (MvQQ) algorithm, in a circumstance of VANET bounded with K-means algorithm clusters which are used for guide assortment for both Personal Best pbest and Global Best*** $g_{best.}$ ***The above can be observed to be a tremendously successful and complete well evaluation of the existing methods.***

Index Terms: ***K-means algorithm, Multivariate Quadratic Quasigroups (MvQQ), Vehicular Ad-Hoc network (VANET).***

I. INTRODUCTION

VANET or Vehicular Ad-Hoc Network is an emerging technology and is a sub-branch of mobile networks, changed in accordance with nodes. It is conceivable that to state a particular occurrence of Mobile Ad-Hoc Network (MANET). A few researchers have determined that the vehicular frameworks are generally called as an Inter-Vehicle Communications (I-V-C), Vehicle-Infrastructure (V-I), Vehicle-Vehicle (V-V), Car-Car (C-C) or essentially VANET. Data are given by the vehicles will be gathered by WAP'S and its aggregate information will be saved as a dynamic server database [1]. Making intercommunication between the node to avoid accident and comfort journey with safety. Vehicles from out of network shall use sensors for reliable communication with the selected destination, and work as both server and client. A standard VANET environment can be made out of vehicles and infrastructure. Vehicular networks associated with Intelligent Transportation System (ITS) can generate quality results to find answers for traffic issues, progressively giving prompt and reliable data and thus helping traffic issues and safety.

This innovation supplies few correspondence channels and is isolated into multi-classes like control channel and administration (benefit) channels. The control channel is assigned for performing with the end goal to encourage communication, which normally occurs inside the other administration channels. Despite the fact that DSRC (Dedicated Short Range Communication) devices are approved to change the administration (benefit) channel, they are presumed to continuously monitor the control channel.

The principle motivation behind a VANET is to provide a facility for parkway voyagers with security [2]; consequently one ought to underscore the significance of giving security to the information movements on this kind of ad-hoc system. Here we suggest that there is a requirement to guarantee that sort of data, particularity for VANET, it is the foundation of a protected association in a brief timeframe, giving high portability for the nodes. In this study, we use an asymmetric encryption algorithm, more specifically, Multivariate Quadratic Quasigroups (MvQQ).

II. INTERCONNECTED WORK

Security in VANETs has been generally contemplated for some researchers, yet the greater part of them do not present data about execution (implementation) or assessment (evaluation) of symmetric or asymmetric algorithms working in a genuine situation of the vehicular network. Consequently, in our insight (knowledge), this paper shows the worth examination and demonstrates the execution time of MvQQ algorithm in different scenarios of VANET. [3] The objective was to accomplish nearby security by utilizing locally available radar to recognize neighbors and to affirm their declared GPS feed. Every vehicle produces data about the condition and movement and dependent on both what is seen? And what is received? from different vehicles in the chosen framework. [4] Vehicular networks won't just give well-being and life-saving applications; however, they will end up being a ground-breaking specialized instrument for their clients. In this examination [4] they assessed the institutionalization execution; moreover, the researchers conducted attempts on vehicular systems contemplated the difficulties of facing future vehicular systems. [5] The authors affirm that the effective organization of vehicular transmission expects the Vehicle-Vehicle (V-V) and Vehicle-Infrastructure (V-I) can affect progress on communication wrapped with security to roadside with safety and traffic. The strategy utilized for secure transmission within the sight of adversaries is known as Cryptography. Cryptography assigns to encryption in which a plaintext message is translated into a ciphertext message and this can be done with a private-key or (public) open-key. Also, the three primary cryptography designs were researched: Open key, symmetric key, and identification based cryptography, which is utilized for the security of the system. [6] Suggested a new grouping model for power transmission among the VANET and to build it alongside the security algorithms with the goal.

Revised Manuscript Received on May 06, 2019

K. Selvakumar, Dept. of Information Technology, Annamalai University, Chidambaram, Tamil Nadu, India

S. Naveen Kumar, Dept. of Computer Science and Engineering, Annamalai University, Chidambaram, Tamil Nadu, India

Shaji. K. A. Theodore, Faculty Information Technology, AI Musanna College of Technology, Oman,

Also, the transmission among the VANET nodes can be made progressively ineffective way. They actualized and determined an arrangement of encryption keys that are utilized to encrypt the following packet from part of the information in the present packet. Here we (the author) are going to display the effect on the Throughput, Success ratio, Handover traffic, and End-to-End delay.

III. K-MEANS CLUSTERING ALGORITHM

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 [8], mainly aims to demonstrate the connection between the nodes to conveys which is best using both Personal Best (p_{best}) and Global Best(pbest) to have more effective and perform all around contrasted with the displayed techniques [9].

A. Personal Best (p_{best}):

The individual best position identified to the particle i is the best detect that the particle has visited (a past estimation of x_i), yielding the best wellness value for that particle. The symbol f(X) will be utilized to mean the objective utility that is being limited. The revised equation is

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

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

B. Global Best (g_{best}):

The g_{best} offers a quicker rate of the union at the expense of robustness. This g_{best} maintains only a single best arrangement called the global best speck, over the total particle in the swarm.

IV. ASYMMETRIC ALGORITHMS

Late investigations display to use asymmetric encryption in embedded systems, as it is insisted by Ref [7], who assessed the asymmetric encryption algorithms with more security levels, as with a key to RSA contains 3076 bits and ECC contains 521 bits in embedded systems.

A.MvQQ Algorithm:

The encryption algorithms beforehand presented the security subject to computationally separated numerical issues, in the year 2008 another plan of an open key was made, known Multivariate Quadric Quasigroups (MvQQ). In Ref [10], this algorithm depends on the quadratic multivariate polynomials and quasigroups changes, holding the accompanying characteristics i.e.

Step 1: considering as out-quantum algorithm;

Step 2: In the encryption methodology, the speed is similar to other open key encryption process subjected to multivariate quadrics;

Step 3: In the decryption, the speed counterparts to commonplace encryption for a symmetric block.

Step 4: Exceedingly parallelizes, dissimilar to different algorithms which are fundamentally progressive. The conventional detail of the MVQQ scheme is a typical 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 quadric 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 $s = (s_1 \ldots\ldots\ldots s_n)$, in other words, r = B(s).

Which can be represented as r, $r = B(s) \equiv y \equiv DZ$

As shown by Ref [7] tests performed on equipment exhibit that MvQQ consists of average symmetric block encryption. In Ref. [13] the analysis with a network of sensors, launch that MvQQ is a couple of sizes quicker than the algorithms like RSA and ECC.

This reality certifies that the outcomes gained in Ref [10] while programming contemplated that the digital signature made by MvQQ is 300 to 70000 times faster than the digital signature delivered by RSA and ECC. In any case, the dominance of MvQQ can accomplish 10000 times. In addition, as shown by Ref [12], that the MvQQ algorithm gives another way for the cryptography field; in general it develops new encryption systems for an open key, and in addition upgrading the existing ones. More insights into these three algorithms (RSA, ECC, and MvQQ) are introduced and considered in Ref [14], [15]. By utilizing these three principles by connecting with its preparing time, storage and processor utilization. The outcomes demonstrated that MvQQ is a decent algorithm for embedded systems which are superior to ECC and RSA.

V. PROPOSED PROTOCOL ARCHITECTURE

In the proposed protocol, a user node needs to commune with another node and can send the messages to registered with the help of Roadside Unit (RsU) and also using K-means Clustering. We propose the best of nodes that can provide the encryption and decryption keys to the nodes in the environment by using MvQQ algorithm.

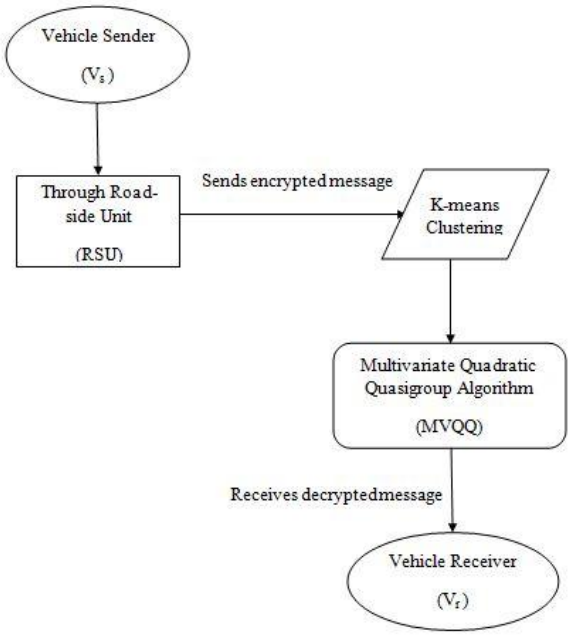

Fig. 1: Proposed Protocol Structure

VI. ANALYSIS AND RESULTS

In this work, the author proposed the actualized and incorporated algorithm MvQQ and K-means Clustering. At that point, information was produced, which enables to gauge algorithm execution on a VANET and perusing the next outcome. It was demonstrated that, in this underlying situation, nodes are found in an area with a little separation not more than 100m. Utilizing a situation of 10 nodes, where node "0" delivers a communicated message to alternate nodes from the network. In our simulations, this procedure happens at an average of 0.4 m. With MvQQ algorithm, the key size is perfect to the others as 160 bits, in such pattern, obviously, it is seen in Figure. 4 a developing curve if the number of information movements in the VANET increments.

Breaking down this outcome, it is conceivable and can obviously understand the MvQQ efficiency against different algorithms. In comparison with the asymmetric algorithms RSA contains 1024-bit with an average of 40ms and ECC contains 192-bit with an average of 10ms and MvQQ with 160-bit also states that the conveyance of the encrypted message is relatively quick. Consequently, MvQQ demonstrates an extraordinary potential, regarding overcome, permitting protected and quick communication. Therefore, the appearance during the investigation accumulated that security level with satisfactory overcome to a VANET situation is undoubtedly an incredible option for secure communications and for vehicular network applications while utilizing an asymmetric algorithm it offers more security levels other than encryption (or) decryption transmission with reliability and authentication. Hence, it appeared in the adequacy of 160bits MvQQ algorithm for encrypted messages conveyance, in spite of the number of digits this message has recommended that MvQQ could be a better option, other than the ECC. Another advantage of this algorithm is the similarity of security level rely upon the measure of the key utilized by the algorithm, sometimes, conveyance times stood near one another. Thus the VANET insists an inside encryption scheme with a lesser security level, is needed from existing, apart from everything else, in the event of conveyance time of the encrypted message.

A. Packet Delivery Ratio (PDR):

The packet delivery ratio is characterized as the entire amount of packets effectively deposited to the entire delivered packets. PDR is described as the number of packets delivered from beginning to end, if the proportion of the network is expanded in any strategy that implies by utilizing this procedure would also improve network assistance. The formula for PDR is:

PDR = (RCV/SND)*100

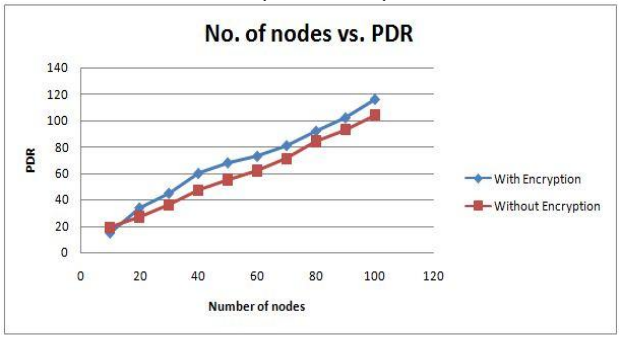

Fig. 2: PDR with respect to nodes with Encryption using MvQQ

In the above diagram, the blue dots demonstrate the proposed line and the red line indicates the existing procedure. The difference can effectively say that the proposed system can produce an improved outcome in contrast with the existing technique.

B. Throughput:

Throughput is a measure of the unit count of data a system can be processed in the given time. It characterizes as the measure of information come truly from a station to another. Bits can also exchange from starting with one place to another in every second. On the off chance that the throughput performances is better than the data transferred between the nodes. Usage shall be better and beneath to noticed value.

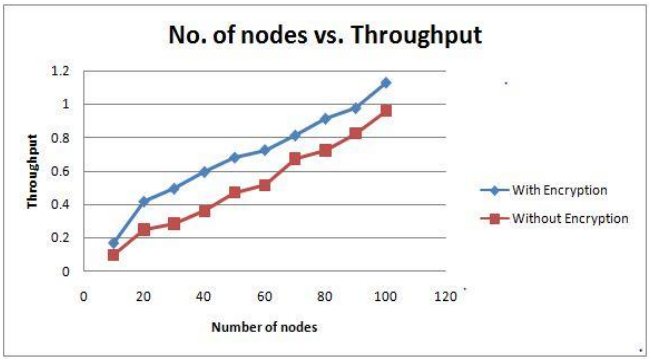

Fig. 3: Throughput performance with respect to nodes with Encryption using MvQQ

In the above graph, blue dots demonstrate the proposed strategy and red dots indicates the execution of the proposed work is high

comparing to the existing procedure.

C. End-to-End Delay:

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

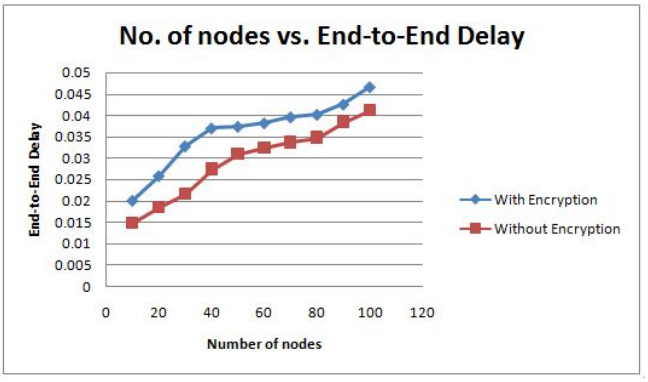

Fig. 4: End-to-End Delay with respect to Time

In the above graph, the encrypted values displayed that the proposed method was increased. Whereas the non-encryption method demonstrates the act of the proposed work is higher as related to the existing method.

D. Packet over Head

The time required 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, the overall transmission speed was decreased due to crude information. Here the graph shows a packet overhead diagram between the current and proposed approach. The proposed methodology is longer in the overhead protocol than the base methodology.

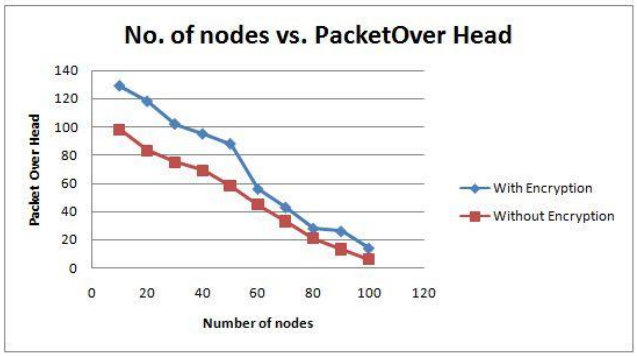

Fig. 5: Packet over Head

A pack of 100 nodes was proposed to the work, the simulation time from one node to another node was observed less. For this situation, the similarity point progresses towards the conveyance time rather than the security level. It is observed that it is not essential that the VANET have a similar key size with a longer security level because the essential characteristics of a VANET are the versatility of each node from the framework while looking for speed and for encryption procedure.

VII. CONCLUSION

The main theme of this paper is to include VANETs and K-means clustering and their response. The current research challenges of VANETs are focused on security. VANET had carried numerous security concerns. The security analysis of our proposed protocol exhibits the elasticity against various security threats. In this paper, the author proposed the MvQQ algorithm for security purposes. Furthermore, the performance appraisal of our proposed protocol could not only display the computational and communication overhead. The approach proposed to minimize the delay and maximize the sanctuary to study the appropriate performance.

REFERENCES

1. M. Azees, P. Vijayakumar, and L. J. Deborah, 2016. ‘‘Comprehensive survey on security services in vehicular ad-hoc networks’’, IET Intell. Transp. Syst., vol. 10, no. 6, pp. 379–388.
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. Abdalla, G.M.T., M.A. Abu-Rgheff, and S.M. Senouci, 2008. “Current trends in Vehicular Ad Hoc networks”, Ubiquitous Comput. Commun. J.
5. Rajni, M.K. and P. Singh, 2013. “An encryption algorithm to evaluate the performance of V2V communication in vanet”, Int. J. Cryptography Inform. Security.
6. 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.
7. Tanwar, G., G. Singh and V. Gaur, 2010. “Secured encryption-concept and challenge”, Int. J. Comput. Applic., 2: 89-94.
8. Nasrin Taherkhani and Samuel Pierre, 2016. “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.
9. Nikhil Padhye, Juergen Branke and Sanaz Mostaghim, 2009. “Empirical Comparison of MOPSO Methods - Guide Selection and Diversity Preservation”.
10. Gligoroski, D., S. Markovski and S. Knapskog, 2008. “A public key block cipher based on multivariate quadratic quasigroups” in Cornell University Library.
11. El-Hadedy, M., D. Gligoroski and S.J. Knapskog, 2008. “High performance implementation of a public key block cipher-MVQQ, for FPGA Platforms” in Sci. Technol..
12. Ahlawat, R., K. Gupta and S.K. Pal, 2009. From MQ to MQQ cryptography: Weaknesses and new solutions. Universia Holding.
13. 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.
14. 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.
15. 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.
16. Rita, 2011. “The Research and Innovative Technology Administration (RITA)”, coordinate the U.S. Department of Transportation’s, 2011.
17. Yanamandram, S., 2009. “Analysis of DSRC based MAC protocols for VANETs. Proceedings of the International Conference on Ultra Modern Telecommunications and Workshops”, Oct. 12-14, IEEE Xplore Press, St. Petersburg, pp: 9-14. DOI: 10.1109/ICUMT.2009.5345593.
18. Edward David Moreno, Leila C.M. Buarque, Florêncio Natan, Gustavo Quirino and Ricardo Salgueiro , “Impact of Asymmetric Encryption Algorithms in a VANET”, at DCOMP/UFS, Universidade Federal de Sergipe, Aracaju/SE-Brasil.

AUTHORS PROFILE

Dr. K. Selvakumar obtained his Bachelor's Degree in Electronics and Communication Engineering in Kongu Engineering College, and the Master's Degree in Communication Systems from NIT Trichy, and Ph.D in Computer Science and Engineering from Annamalai University. He works as Associate Professor in Annamalai University. He has 29years of experience in teaching. His area of interest includes Cryptography and wireless Network, Network Security, Mobile Computing.

S. Naveen Kumar obtained his Bachelor's Degree in Computer Science and Engineering in Annamalai University, and the Master's Degree in Computer Science and Engineering in S.V University, Tirupati. He is currently working towards Ph.D Degree at Annamalai University. His researches interests include Wireless Networks, Vehicular Ad-Hoc Networks, and Network Security.

Author-3
Photo

Shaji K. A. Theodore, working as Faculty in IT, in AI Musanna, College of Technology, Oman.