Asian Journal of Applied Research

ISSN (P):2395-0382, ISSN (O) 2395-1702
Volume: 5, Issue: 1 March 2019
DOI: http://dx.doi.org/10.20468/ajar.2019.1.03

Review Article

Increase the Performance and Security in Vehicular Ad-Hoc Network using Deduction of Sybil Attack

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

[1]*Department of Information Technology, Annamalai University, Chidambaram, Tamil Nadu, India,*
[2]*Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamil Nadu, India*

ABSTRACT

Vehicular ad-hoc network (VANET) was one of the trending and mostly picked research areas for remote sensing applications due to its features such as low-cost assembly, user-friendly, fault identification, fast acquiring of sensed data, and introducing a wide range of sophisticated tools for remote sensing. The sensed data were evolved as a prominent tool to monitor the real-time scenarios to further process of communication and decision-making. In this paper, we propose an asymmetric encryption algorithm with emphasis on Multi-Variate Quadratic Quasigroups (MVQQ) algorithm and also propose the execution examination of the Sybil attack detection in VANET. The execution metric is taken for the assessment of attack which relies on a packet end to end delay, system throughput, and load. This framework was likewise used to counteract Sybil attack by limiting timestamps given by Roadside Units at a beginning stage itself. An attacker is one of the sorts of end client, yet their role in the system is negative and makes issues for different segments of the system. A serious attack, known as Sybil attack, against ad-hoc networks includes an attacker misguidedly asserting numerous characters. A Sybil attack delivers different messages to different nodes. Every in this paper, we discuss some of the techniques put forwarded by researchers to detect Sybil attack in VANET. In this paper, we have discussed about the loom for detecting Sybil attack in VANET using neighborhood-based method. The simulation setup contains 100 vehicular nodes moving with a consistent speed of 10 m every second. The information rate of vehicular nodes is 10 Mbps with default transmitting intensity of 0.006 watts.

Address for correspondence:
K. Selvakumar,
Department of Information Technology, Annamalai University, Chidambaram, Tamil Nadu, India.
Phone: 9443185363,
E-mail: kskaucse@gmail.com

Keywords:
Multivariate quadratic quasigroups, Sybil attack, Vehicular ad-hoc network

Received: 04th February 2019
Accepted: 13th February 2019
Published: 07th March 2019

INTRODUCTION

The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moving cars as nodes in a network to create a mobile network. 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] Their making an intercommunication network between the nodes because of avoiding accidents and make their journey comfort and safely. In a radio communication band, at least multinodes or an intelligent transportation system stations may consequently interface, making an ad-hoc network, which implies that all stations knew 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: On-Board Unit, RsU, and the 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 quasigroups (MVQQ). It also provides other effects such as authenticating user, producing and distributing certificates, and maintaining, managing, and revoking certificates. Open key infrastructure (OKI) is an infrastructure in which various impacts occur and are not a route or algorithm itself, so OKI comprises various perspectives to enable the infrastructure to work.

The principle motivation behind a VANET is to outfit parkway voyagers with security;[3] consequently, one ought to underscore the significance of giving security to the information movements on this kind ad-hoc system that suggests the requirement to guarantee to sort of data. The disposition of a VANET is the establishment of an ensured

relationship association in a brief timeframe, given the high movability of the nodes. In this study, we use asymmetric encryption algorithm, more specifically, MultiVariate Quadratic Quasigroups (MVQQ).

However, a significant problem issue emerges when a pernicious node can imagine as different nodes called a Sybil attack[4-5] and reasonably reinforce false information. On the off chance that favorable elements cannot perceive a Sybil attack, they will trust the false data and base their choices on it. Subsequently, tending to this issue is vital to useful vehicular system frameworks.

INTERCONNECTED WORK

Security in VANETs has been generally contemplated for some researchers, yet the greater part of them does not show the data about execution or assessment of symmetric or asymmetric algorithms processing in a genuine situation of the vehicular system. Consequently, in our insight, this paper shows the worth examination since it demonstrates the execution time of MVQQ algorithm in different scenarios of VANET.[6] The objective was to accomplish nearby security by utilizing locally available radar to recognize neighbors and to affirm their declared GPS organizes. Every vehicle produces data about the condition of the movement dependent on both what is seen and what is received from different vehicles in the framework.[7] Vehicular networks would not 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, they assessed the institutionalization execution and researcher's connected attempts to vehicular systems are discussed, and the difficulties facing future vehicular systems are also explained.[8] The authors affirm that the effective organization of vehicular transmission expects the Vehicle-with-Vehicle (V-V) and Vehicle-with-Infrastructure (V-I) transmission with security to roadside protection and traffic. The technique utilized for secured transmission inside the sight of adversaries is known as cryptography. Cryptography assigns to encryption in which a plaintext message is converted into a ciphertext message and should be possible with a private key or open key. Furthermore, the three primary cryptography designs were researched: Open key, symmetric key, and identification-based cryptography, which are utilized for the security of the system.[9] Suggested the recent grouping ideal for powerful transmission among the VANET and to build it alongside the security algorithms with the goal that the transmission among the VANET nodes can be made progressively effective 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. In this paper, we endeavored to protect against the Sybil attack with just help of RsUs. At whatever point a node passes the RsUs, it acquires a timestamp. It is troublesome for multinodes to acquire the equivalent timestamp while crossing various RSUs. Due to giving different timestamps, it is unreliable for any attack. At the point, when a node asks for different timestamps from a solitary RsUs, it implies quite possibly that the node may go about as a Sybil attacker.[10]

SECURITY IN VANET

Late investigations display to use asymmetric encryption in the embedded systems, as it is insisted by[13] who assessed the asymmetric encryption algorithms with more security levels, RSAs with a key size to 3076 bits, and ECCs with a key size to 512 bits in the embedded systems.[11]

Asymmetric algorithm

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 the open key was made, known as MVQQ. In a study of Gligoroski,[14] this algorithm depends on the quadratic multivariate polynomials' and quasigroups' changes and holds the following accompanying characteristics.

- This is an out-quantum algorithm;
- In the encryption methodology, the speed is similar to another open key encryption processes subjected to multivariate quadratics;
- In the decryption, the speed counterparts to a commonplace encryption of a symmetric area;

The conventional detail of the MVQQ design is a common multivariate quadric system.

$$AoBoC: \{0,1\}^n \rightarrow \{0,1\}^n$$

Where A and C are multi non-singular linear transformations, and 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.

$B = \{Bi(s_{1\ldots\ldots} s_2) \mid i = 1,\ldots,n\}$ Over the vector $s = (s_1 \ldots\ldots\ldots s_n)$, in other words, r = B (s).

What can be represented as,

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

As shown by Huang,[13] tests performed in equipment exhibit that MVQQ consists of an average symmetric block encryption. In a study of Maia,[15] investigations with a framework of sensors launch that MVQQ is a couple of sizes quicker than the algorithms such as RSAs and ECCs. This reality certified that the outcomes gained in a study of Gligoroski[14] while using programming; he contemplated that the digital signature made by MVQQ is 400–60,000 times quicker than RSA and ECC digital signature. In any case, the dominance of MVQQ can accomplish 10,000 times. In addition, as shown by Ahlawat,[16] 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.[17,18] They have utilized 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 ECCs and RSAs.[12-18]

ATTACKS IN VANET

Attacks in VANET: The security in VANET is mainly used for controlling of accidents, traffic, and executives of parking in open region. In VANET's, the different noteworthy worries are protection and security.

Security in VANET

Late investigations displays that the use of an asymmetric encryption in the embedded systems, as it is insisted by[10]. It also assessed the asymmetric encryption algorithms with more security levels as which the RSA contains a key-size of 3076 bits and ECC contains the key-size of 512 bits in the network.

In VANETs, the different noteworthy worries are protection and security. Deplorably, in VANETs, most security protecting plans are powerless against Sybil attack.

Sybil attack

A Sybil attack is caused in VANET when a malicious node or RsU can obtain numerous characters. A Sybil attacker sends various messages with a particular false personality to different nodes in line. This makes a deception (or) confusion to other nodes in the similar path. It contains different sorts of nodes [Figure 1].[19-22]

(a) Pernicious node/Sybil attacker: The node which spoofs the personalities of different nodes.
(b) Sybil node: The new characters made by the pernicious node to attack are known as Sybil nodes.

Figure 2 demonstrates Sybil attacks in VANET are mainly spoofs the personalities of S1, S2, and S3. Sybil attack is spoofing the personalities of S1, S2, and S3. The effect of Sybil attack gets severe serious when all characters made by attacker take an interest at the same time in the system. Sybil attack is grouped into two classes. The two are clarified as follows:

Step 1: The Sybil attacker makes the characters of the real current nodes in the system. Let W be the arrangement of all nodes in VANET, and Y be the arrangement of all Sybil nodes. For this situation, ($Y \subseteq W$) (1)
Step 2: The Sybil attacker makes the characters from outside the system. For this situation, ($Y \not\subset W$) (2)

The Sybil attack makes diverse identities appropriate on time since each node is confirmed correspondingly with its open key.

In this attack, attacker makes diverse identities to reestablishing distinctive focuses. This attack is an intense attack in which a node can assert at better places with a few fake characters in the meantime and make enormous security hazards in the framework. A Sybil attack is unsafe for framework topologies and associations and in addition framework transmission capacity utilization. In this Figure 2, an attacker S1 exchanges numerous messages with various characters to alternate nodes.

In Figure 3, it describe as the quantity of packets is deliver from origin to terminal if the proportion of the network is expanded in any strategy that implies by utilizing this procedure network assistance improves. As the use of this encryption method it slightly reduces the malicious attacks from the network region for the communication purpose between the nodes.

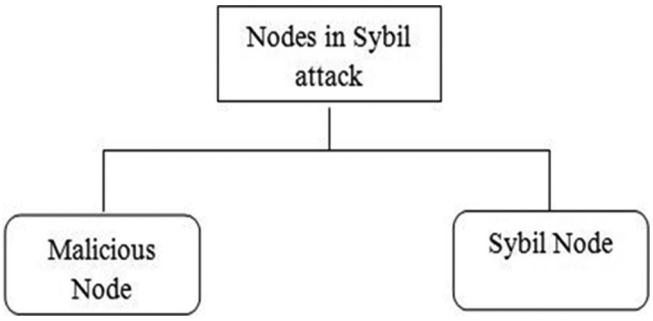

Figure 1: Nodes participates in Sybil attack

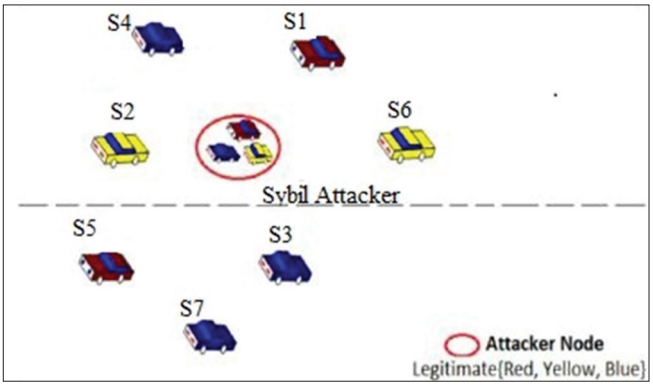

Figure 2: Sybil attack in vehicular ad-hoc network

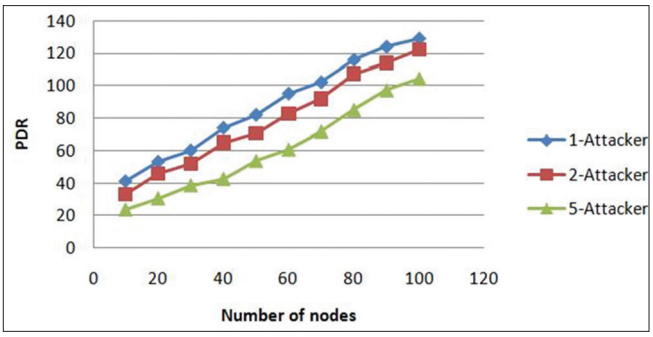

Figure 3: Packet delivery ratio with respect to nodes

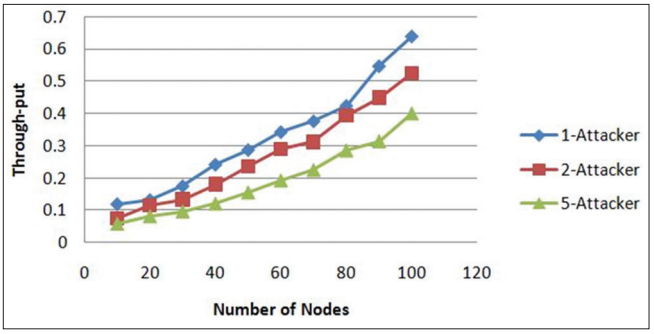

Figure 4: Throughput with respect to nodes

NETWORK SIMULATION

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 peruse the outcome next. Here, we can see that, in this underlying situation, nodes are found in an area with a separation littler than 100 m. In our simulations, this procedure happens on an average of 0.4 m.

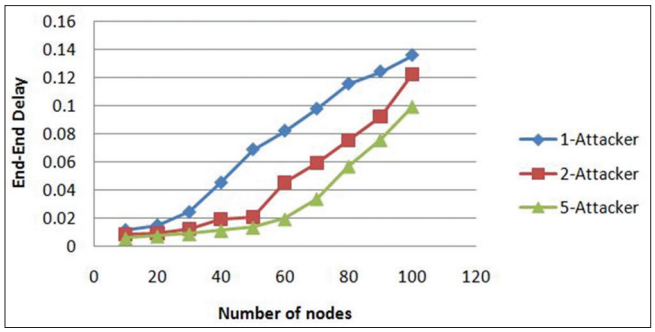

Figure 5: End-to- end delay with respect to nodes

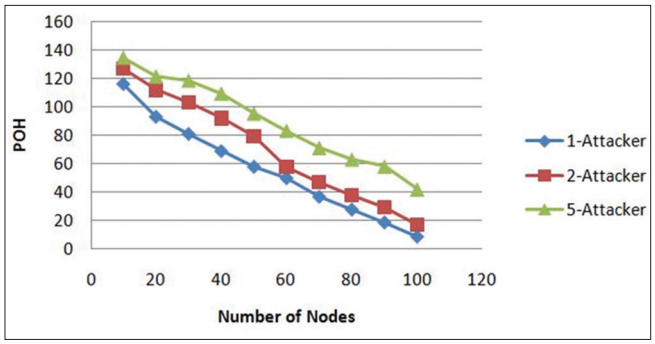

Figure 6: Packet overhead with respect to nodes

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, and 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 assessed the execution of RsUs if the node significantly asks the RsUs 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 RsUs can essentially check whether it is capable to implement this task on a persistent condition to the nodes.

Results are obtained in the case of the simulations reflective in the Figure 5, it depicts the quantum of nodes significantly differences in the condition for the proposed encryption process. It also shows the slight differences between the nodes from 2-attacker to 5-attacker when the node is in the position of 0.1m.

Packet delivery ratio (PDR)

PDR is described as the extent of quality of information packets sent by the source node and the amount of packets get by the destination node.

PDR = (received packets/packets sent)*100

Throughput

It is portrayed as the successful data or information packets transmitted per unit time. The parameter varies explicitly with the quantity of packets got and is reverse relative comparing to the end-end delay.

Throughput = Σ received packets/(arrived time send time)*packet size*time/1000 in kbps.

End-end delay

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

$d_{end\text{-}end} = M (d_{commn} + d_{proc} + d_{proc} + d_{queue})$

Where

d_{commn} = communication delay

d_{proc} = propagation delay

d_{proc} = process delay

d_{queue} = Queue delay

M = Number of links (Number of router -1).

Packet overhead

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, Figure 6 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.

CONCLUSION

The current research challenges of VANETs are focused on security. VANET carries numerous security concerns. The security investigation of our proposed convention exhibits the elasticity against different security warnings. In this survey article, we have presented security measures to be taken before implementing a VANET. 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. By attack counteractive action component, the Sybil attack itself starts the timestamps. In future, we will counteract attack, without confining the arrangement of timestamps to nodes, and limit the calculation effort of algorithm. As we increment a number of nodes, it might outcome in more defer which builds the bottlenecks in system correspondence.

REFERENCES

1. Khan PA. Security of Self Organizing Networks: MANET, WSN, WMN, VANET. International Standard Book No. 13-978-1-4398-1920-3. CRC Press; 2011.
2. Sumra IA, Hasbullah HB, Manan J, Lail A. Comparative study of security hardware modules (EDR, TPD and TPM) in VANET. 3rd National Information Technology Symposium (NITS 2011). Riyadh: King Saud University Riyadh; 2011.
3. Patel ST, Mistry NH. A Review on Sybil Attack Detection Techniques in WSN. In 4th International Conference on Electronics and Communication Systems (ICECS); 2017.
4. Kamani J, Parikh D. A review on Sybil attack detection techniques.

J Res 2015;1:27-31.
5. Karn CK, Gupta CP. A survey on vanets security attacks and Sybil attack detection. Int J Sens Wirel Commun Control 2016;6:45-62.
6. Kafil P, Fathy M, Lighvan MZ. Modeling Sybil Attacker Behavior in VANETs. Information Security and Cryptology (ISCISC). 2012 9th International ISC Conference. IEEE; 2012. p. 162-8.
7. Choudhary GK. Providing VANET Security through Position Verification. M.Sc., Thesis. Norfolk: Old Dominion University; 2007.
8. Rajni MK, Singh P. An encryption algorithm to evaluate performance of V2V communication in vanet. Int J Cryptogr Inform Secur 2013;3:15-22.
9. Bhuvaneshwari S, Divya G, Kirithika KB, Nithya S. A novel approach for secured data transmission in VANET through clustering. Int J Electron Commun Eng 2014;9:23-30.
10. Huang JL, Yeh LY, Chien HY. ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Trans Veh Technol 2011;60:248-62.
11. Gligoroski D, Markovski S, Knapskog S. A Public Key Block Cipher Based on Multivariate Quadratic Quasi Groups. Cambridge: Cornell University Library; 2008.
12. Maia RJ, Barreto PS, Oliveira BT. Implementation of multivariate quadratic quasigroup for wireless sensor network. Trans Comput Sci 2010;6480:64-78.
13. Ahlawat R, Gupta K, Pal SK. From MQ to MQQ Cryptography: Weaknesses and New Solutions. New Delhi: Universia Holding; 2009.
14. Quirino G, Moreno E. Architectural evaluation of asymmetric algorithms in ARM processors. Int J Electron Electrical Eng 2013a;1:39-43.
15. Quirino G Moreno E. Architectural evaluation of algorithms RSA, ECC and MQQ in ARM processors. Int J Comput Netw Commun 2013b;5:153-68.
16. Hoa LA, Cavalli A. security attacks and solutions in vehicular ad hoc networks: A survey. International Journal on AdHoc Networking Systems 2014;4:1-20.
17. Kumar PV, Maheswari M. Prevention of Sybil attack and priority batch verification in VANETs. Chennai, India: ICICEs; 2014.
18. Hamed H, Keshavarz-Haddad A, Haghighi SG. Sybil Attack Detection in Urban VANETs Based on RSU Support. In 26th Iranian Conference on Electrical Engineering (ICEE); 2018.
19. Soni M, Jain A. Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks. In Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC); 2018.

Cite this article: Selvakumar K, Naveen Kumar S. Increase the Performance and Security in Vehicular Ad-Hoc Network using Deduction of Sybil Attack. J Appl Res 2019;5(1):17-21.

Source of Support: Nil, **Conflict of Interest:** None declared.