Journal of Computer Sciences

Original Research Paper

Impact of Asymmetric Encryption Algorithms in a VANET

Edward David Moreno, Leila C.M. Buarque, Florêncio Natan, Gustavo Quirino and Ricardo Salgueiro

DCOMP/UFS, Universidade Federal de Sergipe, Aracaju/SE-Brasil

Article history
Received: 30-10-2014
Revised: 15-05-2015
Accepted: 28-12-2015

Corresponding Author:
Edward David Moreno
DCOMP/UFS, Federal University of Sergipe, Aracaju/SE, Brazil
Email: edwdavid@gmail.com

Abstract: This paper describes the impact of using asymmetric encryption algorithms, with emphasis on RSA, ECC and Multivariate Quadratic Quasigroup (MQQ) algorithms, in a scenario of Vehicular *Ad hoc* Network (VANET). In the research we used the simulator NS-3 with specific module for vehicular networks. The algorithms were implemented in C and were included in NS-3. The results, even in a simple scenario of VANET, show that it is possible to add protocol layer security services. We implement and compare three asymmetric algorithms (ECC, RSA and MQQ).

Keywords: RSA, ECC, MQQ Algorithm, Vanets, Simulators, NS-3

Introduction

VANETs or Vehicular *Ad Hoc* networks are mobile networks adapted to vehicles. It is possible to say they are a special case of Mobile Ad Hoc Network (MANET). Some authors have mentioned that vehicular networks are also known as Inter-Vehicle Communications (IVC), Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), Car-to-Car (C2C) or simply VANET. Thus, they are wireless networks among automotive vehicles that present high mobility and well defined routes, given a known source and destination. In this context, new applications have been submitted to this new scenario, seeking for access ubiquity (C2C, 2011). Vehicular networks applied to the ITS might find solutions to traffic problems, dynamically providing immediate reliable information and, consequently, helping traffic safety. As safety on public highways is the main purpose of ITS, in this study it is possible to notice that VANET applications shall provide drivers and pedestrians with a better reliance on travelling for highways.

Ad hoc networks are characterized by being wireless networks in that all of its nodes are effectively active on communications. In other words, they don't need a fixed infra-structure as access points to establish the network. In a radio communication band, two or more vehicles or Intelligent Transportation System (ITS) stations automatically connect, creating an *Ad Hoc* network, this means that all stations know the position, speed and direction of the other stations, becoming capable of providing alerts and information.

This technology was established by Institute of Electrical and Electronic Engineers (IEE) as a new communication pattern between vehicles, namely Wireless Access in Vehicular Environments (WAVE), which groups a family of four protocols dedicated to communication between vehicles, normalized by IEEE 1609. This pattern allows communication to happen only between vehicles or between vehicles and some fixed device on the road, utilizing a 5,9 GHz Dedicated Short Range Communications (DSRC) radio technology, which essentially is a extension of the IEEE 802.11a pattern.

ITS (2011) the family of IEEE 1609 standard defines the architecture, the communication model, the management structure, the security mechanism and the access to the physic layer for high speeds under 27 Mb s^{-1} and small distances until 1000 m and low latency in wireless communication for vehicular environments. It also establishes the basic components of the architecture, namely: On Board Unity (OBU), Road Side Unity (RSU) and the WAVE interface.

This technology supplies several communication channels, which are divided in two categories: Control channel and service channels. The control channel is reserved for broadcasting in order to coordinate communication, which generally happens inside other service channels. Even though DSRC devices are authorized to change to a service channel, they are supposed to continually monitor the control channel. There is no verification and association as there is on the 802.11 standard, where the operations are completed via a signal sent by the RSU inside the control channel.

While OBU and RSU are authorized to transmit messages on control channels, only the RSU should send signaling messages.

In 2004, the IEEE started standardizing Vehicular Network Communications inside the workgroup IEEE 802.11. The IEEE 802.11p WAVE standard stills in development stage (Rita, 2011). In Fig. 1 it is possible to notice the WAVE pattern and the division of the network layers. Specifically, the security services layer (IEEE 1609.2) is where this research aims to assemble an encryption module, with the objective of making a safe VANET communication, free of ordinary attacks to data networks.

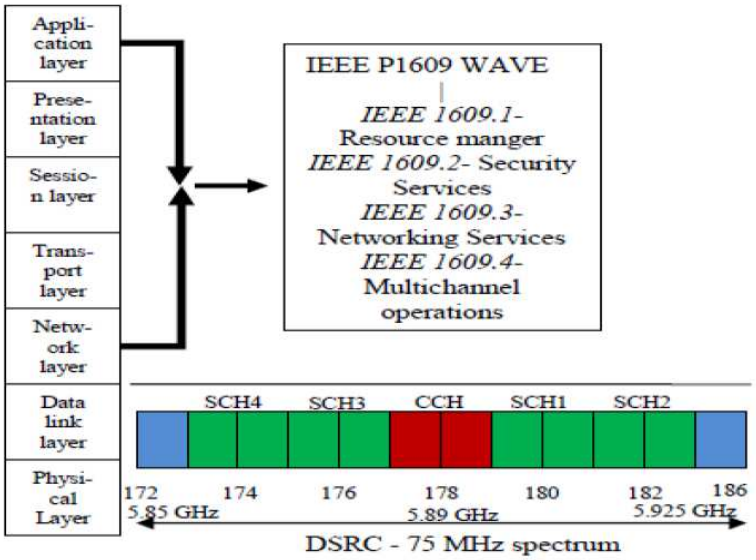


Fig. 1. IEEE WAVE and DSRC (Yanamandram, 2009)

The WAVE architecture is defined in six documents (ITS, 2011): IEEE P1609.1, IEEE P1609.2, IEEE P1609.3, IEEE P1609.4, IEEE 802.11e IEEE 802.11p.

The main purpose of a VANET is to provide highway passengers with security (Sumra *et al*., 2011); hence one should emphasize the importance of providing security to the data that travels on this type of *ad hoc* network, which implies that there is a need to protect that kind of information. The particularity of a VANET is the establishment of a safe connection in a short period of time, given the high mobility of the nodes. In other side, it is very well known that asymmetric algorithms need more processing and it is critical in embedded systems and in our case, in vehicular networks. Thus, in this study, we use asymmetric encryption algorithms, more specifically, the Rivest, Shamir and Adleman (RSA), Elliptic Curve Cryptography (ECC) and Multivariate Quadratic Quasigroup (MQQ). These algorithms were implemented in C and included in the NS-3 simulator.

Therefore, this paper presents results obtained inside a VANET simulation environment using NS-3, where it was created a simple scenario of a vehicular network, with only ten nodes which are receiving an encrypted message broadcasted from one VANET´s node and they should decipher this message after received.

Asymmetric Algorithms

Recent studies indicate that it is possible to utilize asymmetric encryption in embedded systems, as it is confirmed by (Tanwar *et al*., 2010) who evaluated asymmetric encryption algorithms with high security levels, RSA with a key to 3076 bits and ECC with key to 521 bits in embedded systems.

RSA Algorithm

Rivest *et al*. (1978) the authors proposed a method to implement an encryption system with public key, whose security lies on the difficulty of factoring big integer numbers. Through this technique it is possible to encrypt data, as well as creating digital signatures. Nowadays, the RSA is the most used public key algorithm around the globe. The algorithms for generating public and private keys, used to encrypt end decrypt messages, use the pair (n,e) which is the public key and the pair (n,d) as the private key. The process for encryption and decryption are shown in Algorithm 1 and 2.

Algorithm 1: RSA Encryption
Input: RSA Public key (n,e), raw text m $\in$ [0, n-1]
Output: Encrypted Text c begin
1. Compute $c = m^e \bmod n$
2. Return c.
end.

Algorithm 2: RSA Decryption
Input: RSA Public key (n,e), RSA Private key (n,d), encrypted Text c
Output: Raw Text m begin
1. Compute $m = c^d \bmod n$
2. Return m.
end.

ECC Algorithm

In the mid-80's (Koblitz, 1987; Miller, 1986) proposed an encryption method based on elliptic curves Elliptic Curve Cryptography (ECC). According to ECC's creators, an elliptic curve is a plain curve defined by the following

equation: y2 x3 + ax + b. The efficiency of this algorithm is based on finding a discrete logarithm of a random element, which belongs to an elliptic curve. In order to get an idea of the applicability of elliptic curves-based algorithms, in devices with computational restrictions, Chatterjee *et al.* (2011) mention that the efficiency of the ECC encryption algorithm, with keys to approximately 160 bits, is the same obtained from the RSA algorithm with a 1024-bit key. Algorithms from several functionalities are based on elliptic curves, including key management, encryption and digital signature.

The main idea of this algorithm is to construct a set of points of an elliptic curve in that the logarithm problem is unapproachable. According to (Blake *et al*., 1999) cryptographic systems based on elliptic curves reach the same security level of RSA-based security systems, utilizing smaller keys, hence consuming less memory resources and processor. This makes its usage ideal for smart cards and other environments where resources like storage, time and power consumption are restricted.

Encryption and decryption procedures using elliptic curves are similar to the ElGamal encryption scheme and they are described in the algorithms 3 and 4.

Algorithm 3: ElGamal *Elliptic Curve Encryption*
Input: Parameters from the elliptic curve domain (p, E, P, n), Public Key Q, Raw Text m
Output: Encrypted text (C1, C2) begin
1. Represent the message m as a point M in E(Fp)
2. Select k ∈R[1,n−1].
3. Calculate C1 = kP
4. Calculate C2 = M + kQ.
5. Return (C1, C2)
end.

Algorithm 4: ElGamal *Elliptic Curve Decryption*
Input: Parameters from the elliptic curve domain (p, E, P, n), Preavete key d, Encrypted text (C1, C2)
Output: Raw Text m begin
1. Calculate M = C2- dC1 and extract m from M.
2. Return (m).
end.

The raw text m is firstly represented as a point M and then it is encrypted by adding kQ, where k is a randomly chosen integer and Q is the public key (Hankerson *et al*., 2004). The broadcaster transmits the points C1 = kP eC2 and eC2 = M + kQ to the receiver, which uses its private key to calculate dC1 = d(kP) = k(dP) = kQ and then compute M = C2 − kQ. An intruder who wishes to read M needs to calculate kQ.

The model of this algorithm has been quite studied because, according to (Amin *et al*., 2008), in the last years the ECC has called attention as the security solution for *Ad Hoc* networks, due to its usage of small keys and low computational *overhead.*

MQQ Algorithm

The encryption algorithms previously presented have their security based on computationally unapproachable mathematical problems: Computational efficiency of the discrete logarithm calculation and integer factoring.

In 2008 a new scheme of public key was created, called Multivariate Quadric Quasigroup (MQQ). According to Gligoroski *et al*. (2008), this algorithm is based on quadratic multivariate polynomials and quasigroups transformations, holding the following properties: (1) It is a post-quantum algorithm; (2) In the encryption process, its speed is comparable to other public key encryption systems based on multivariate quadrics; (3) In the decryption, the speed equals to a typical encryption of a symmetric block and (4) highly parallelizable, unlike other algorithms which are essentially sequential.

A generic description for the MQQ scheme is a typical multivariate quadric system T o P o S: $\{0,1\}^n \rightarrow \{0,1\}^n$ where T and S are two non-singular linear transformations and P′ is a bijective multivariate quadric mapping over $\{0,1\}^n$. The encryption algorithm with public key is the direct application of a set of n multivariate polynomials $P = \{P_i(x_1,..., x_n) \mid i = 1, ... , n\}$ over the vector $x = (x_1, ... , x_n)$, in other words, $y = P(x)$. What can be represented as $y = P(x) \equiv y \equiv A.X$.

According to El-Hadedy *et al*. (2008) experiments performed in hardware show that MQQ can be as fast as a typical symmetric block encryption. Maia *et al*. (2010), in his experiments with a network of sensors, found that MQQ is several magnitudes faster than algorithms like RSA, DH and ECC. This fact confirmed the results obtained by Gligloroski (2010), when using software, he concluded that the digital signature generated by MQQ is 300 to 70000 times faster than the digital signature generated by RSA and ECC. However, in hardware, the supremacy of MQQ can reach 10.000 times. Moreover, according to Ahlawat *et al*. (2009), the MQQ algorithm gives a new direction for the cryptography field, where it can be utilized to develop new encryption systems of public key, as well as enhancing the existent ones.

More details about these three algorithms (RSA, ECC and MQQ) are presented and analyzed in (Quirino and Moreno, 2013a; 2013b). They have used three criteria by comparison: The processing time, memory and processor usage. They used the Simple Scalar tool for simulations analysis. The results showed that MQQ is a good algorithm for embedded systems since it is better than ECC and RSA. Here, it is important to remind that the ECC is the standard used into VANETS, see the Wave protocol (Rita, 2011; Yanamandram, 2009) and for this reason, we used it as our core and we used the RSA since it was recently used in many platforms and we

used MQQ as future reference, since it is under study and it promises good results.

Simulation Environment

Comparison Among RSA, ECC and MQQ

As these algorithms are asymmetric, they hold the same level of security, besides requiring smaller keys and consuming less computational resources, such as memory, processor and energy, in comparison to other resources that are often utilized by the community. The MQQ with a 160-bit key obtains the same security level of the RSA with a 1024-bit key and ECC with 192 bits. Using the data provided by Table 1, taken from Branovic *et al*. (2004), it is possible to notice.

During the development of this research, it was utilized C programming language, as well as the Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL) library, which is an encryption library in C (Miracl, 2012). These algorithms use complex operations with large numbers, hence it was necessary to use libraries that help and allow these operations. Furthermore, another advantage of utilizing MIRACL is to insert security inside embedded systems. We have developed a implementation of MQQ, following the algorithm specifications and utilizing the Core from Maia *et al*. (2010).

Initially some tests were performed on a desktop, using a simple C and C++ compiler. After the execution, we measured the encryption and decryption time with a fixed 50-digit message. Each execution was performed 10 times, registering the average value from the execution (Fig. 2). In Fig. 2 it is possible to clearly notice the superior performance from de algorithms ECC and MQQ, in comparison to RSA, where MQQ is faster than ECC.

VANET Simulation using NS-3

VANET is a relatively new type of *Ad Hoc* network, consequently there are not enough available VANET devices for easy access, so that experiments from real studies could be done. Vehicular network simulators have been contributing with the progress of VANET researches, as well as developing protocols, applications and the increasing usage of scenarios for vehicular networks with mobility and application validations. According to Martinez *et al.* (2009), network simulators are important because they show us, very detailed, the following: Packages in a simulation level of source, destination, data transmission traffic, acceptance, charge, route, links and channels. Therefore, we have chosen network simulators that were available on the scientific community. Initially, a survey was conducted to learn the available vehicular network simulators that met the research requirement of being open source software.

In this study we studied the TraNS, NSTUns, SUMO, VanetMobiSim and NS-3. When the source codes of these simulators were analyzed with the intention of including security algorithms, it was noticed that, at no time, these codes performed data transfer, in particular, message exchanging between nodes. Although they seemed to exchange messages during the execution of the scenarios we created.

On the specific case of the VanetMobiSim, for instance, each line from the source code was analyzed in detail and instead of sending information to the following node so that an action could be determined, the IDM actually does an proximity test, simulating an effective communication between nodes. Even trying to implement that message exchange in this simulator, we have concluded that this exchange happened instantly, which didn't meet some requirements of a network communication, including sending time, jitter and latency and did not even stored the information exchanged. Therefore, owing to the fact that these simulators do not allow data exchange, it was not possible to include encryption algorithms satisfactory and consequently we decided not to work with them in this study.

The only simulator which allowed insertion and analysis of encryption algorithms was the NS-3. Initially, it was intended to install NS-3 in a Windows platform, however, the simulator developer himself, suggests it to be installed by a virtualization process in a Linux distribution with NS-3. Thus, we created two simulation environments with the NS- 3, one is a virtual machine and the other is a desktop. Both of them obtained a good performance.

With NS-3 it was possible to create a determined scenario and test a real communication between nodes. This allowed an analysis of performance of the algorithms inside a VANET simulator, which is one of the challenges of this research.

Inclusion of Security Algorithms in NS-3

In order to make it possible to create a simulation of mobility using NS-3, it is necessary to install an extra module to the simulator, which is called “NS-3-highwaymobility”, responsible for traffic generation and control, because NS-3 is a network simulator not specialized in VANET networks. This module is installed by copying the folder that contains its source code and then, typing the command line “bld.add_subdirs (‘vanet-highway’);” to the NS-3 settings script (wscript).

The command line has to be typed on the section initiated by “# process subfolders from here”. After installing the first mobility module so that encryption algorithms work, firstly, it is necessary to add the Miracl library to the wscript inside NS-3 folder using the command line “conf.env.append_value ('LINKFLAGS’,’ <path to the installed library >);”.

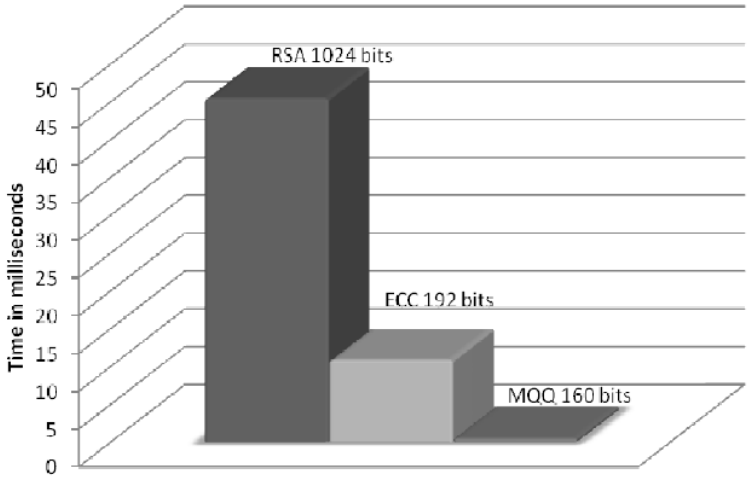
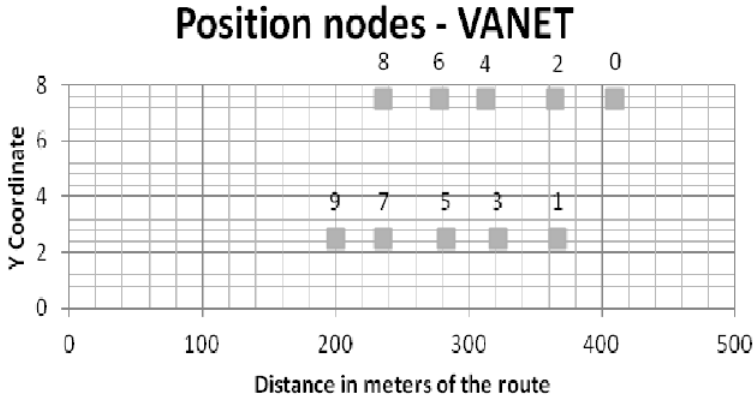
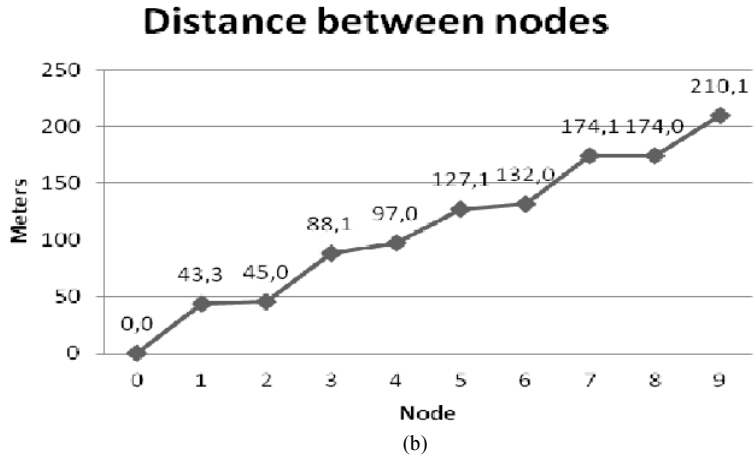


Fig. 2. Execution Time of the Algorithms RSA, ECC and MQQ on a desktop



(a)



(b)

Fig. 3. (a) Scenario of a VANET on NS-3 and (b) Real distance among nodes

Table 1. Equivalent keys in bits for RSA-ECC-MQQ

RSA	1024	2048	3072	7680	15360
ECC	192	224	256	384	521
MQQ	160	160	—	—	—

The command line has to be typed before the section "# Write a summary of optional features status". After the inclusion of Miracl library, the algorithms subjects to study must be added to the project "vanet-highway" by editing wscript file contained in the folder of same

name, adding the variable "obj.source" and the names of the source files of the algorithms (NS3, 2012; NS3hm, 2012).

After these modifications the code must be recompiled, for this, it is necessary to open a terminal screen and change the actual directory to the directory where NS-3 is installed and type the following command line: "*./waf --run 'vanethighway-test --project=./vanethighway/Examples/SimpleStraightHighway.xml-- enablevehiclereceive=1'* ". Besides recompiling the simulator, one should do the same for the example project that comes with the "ns-3-highway-mobility".

Scenario of Our Tests

Overall, we used three simple scenarios which utilized (using 10, 30 and 50 vehicles, respectively) with the only objective of travelling data in a simple, but safe way. It was decided to establish some basic parameters in the settings file (xml) on NS-3. For the roads, we choose 01 highway, with 2, 12 and 20 bands, in a unique way. By the time vehicles enter a highway, the first node, referred as node "0" by this study, sends a broadcast message to the other nodes that are entering the highway. This message may be an alert, a collision or a malfunction of a vehicle in the middle of the road. This message can contain normal text message characters, so drivers from other vehicles may be informed of an accident. What to do with the information sent and received by other nodes depends on the application a VANET is designed for. This is not the focus of this work, which aims the information exchange between nodes of a VANET, offering security during this message exchange.

Thus, a determined message was encrypted by the source node (encrypted using the selected algorithm) and once it is received by a node, it must be decrypted in the place the message is received. This was verified and works fine.

Other parameters of the scenario configuration were the definition of the wi-fi 802.11a, the 10MHz frequency and the traffic rate of 6 MB s^{-1}, the initial distance between nodes varies from 39 m to 45 m, the minimum speed was 65 km h^{-1} and the maximum was 80 km h^{-1}. Figure 3 shows node position inside the simulation scenario utilized in this article. It's worth highlighting that this figure was generated during the simulation, where effectively, there is a dispatch and a receipt of a message encrypted by a transmitter node, received and decrypted by the other nodes.

In Fig. 3, a message varies from 06 to 60 digits on each simulation. This message size was adopted because we understand that in a vehicular network, there is no need to exchange large messages, as the main objective of a VANET is exchanging basic information of traffic control and security on public highways, with high mobility between the nodes. The larger the message is, more time is required for exchanging data between nodes.

Results and Analysis

As proposed by this work, we implemented and included the algorithms RSA, ECC and MQQ in the NS-3 simulator. Then some data was generated, which allowed us to measure algorithm performance on a VANET and reading the results later. As shown in Fig. 6, it is possible to see node position at the moment there is a encrypted message delivery, so in Fig. 6 it is also possible to observe the real distance between nodes at this exact moment. In Fig. 4, one can observe that, in this initial scenario, nodes are found in a region with a distance smaller than 250 m. One can observe that as the nodes are inside the network range, there was no package discard. Using a scenario of 10 nodes, where node "0" sends a broadcast message to the other nodes from the network. After that, we present algorithm performance with key size variations.

Figure 4 shows the delivery of a 60-bit message (~8 characters) encrypted with RSA and a key variation between 16 and 1024 bits. It is possible do observe in the Fig. 4 that in the case of using RSA with keys varying from 16 to 254 bits, there is a high proximity of time from a safe communication (compounded by message encrypt + VANET message deliver + acceptance of the message by the node that receives the encrypted message).

A 512-bit key can also be suggested when it is wanted less runtime and more security, because delivery time stays, on average, 6 m slower than a 256-bit key. However, a 1024-bit key requires a longer runtime to process encrypt/dispatch + receipt/decrypt, in the graph it is around 40 m, which corresponds to simple scenario featuring 10 nodes, with the same characteristics previously described, nodes varying from 65 to 80 Km h^{-1} and in a region of 300 m.

In the Fig. 4, it is possible to see that this time is 40 m, which means a raise of 40 times when compared to 12-bit keys. As expected, when more security is desired, it is necessary to increase key size, which means more time to decide between security levels versus runtime.

Figure 5 depicts the communication time for distinct key sizes, using the ECC and MQQ. With this ECC algorithm it is possible to realize a better performance with a 16-bit key, as shown by the Figure. However, when compared by the same security level of a 1024-bit RSA, which equals to a 192-bit ECC, we perceived a safe communication time of 12 ms, in comparison to 42 m from 1024-bit RSA, which means that it is 3.5 times faster. In a similar way, Fig. 5b depicts safe communication time using MQQ. In our simulations, this process occurs on average 0.4 m. Hence we highlight the efficiency of MQQ, according to what has been tested by other works previously mentioned, but in different contexts of VANET networks.

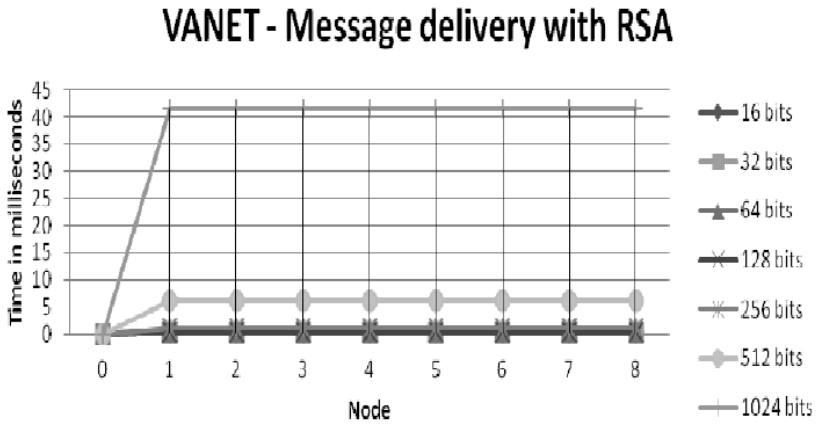


Fig. 4. Time of a communication in Vanet with RSA

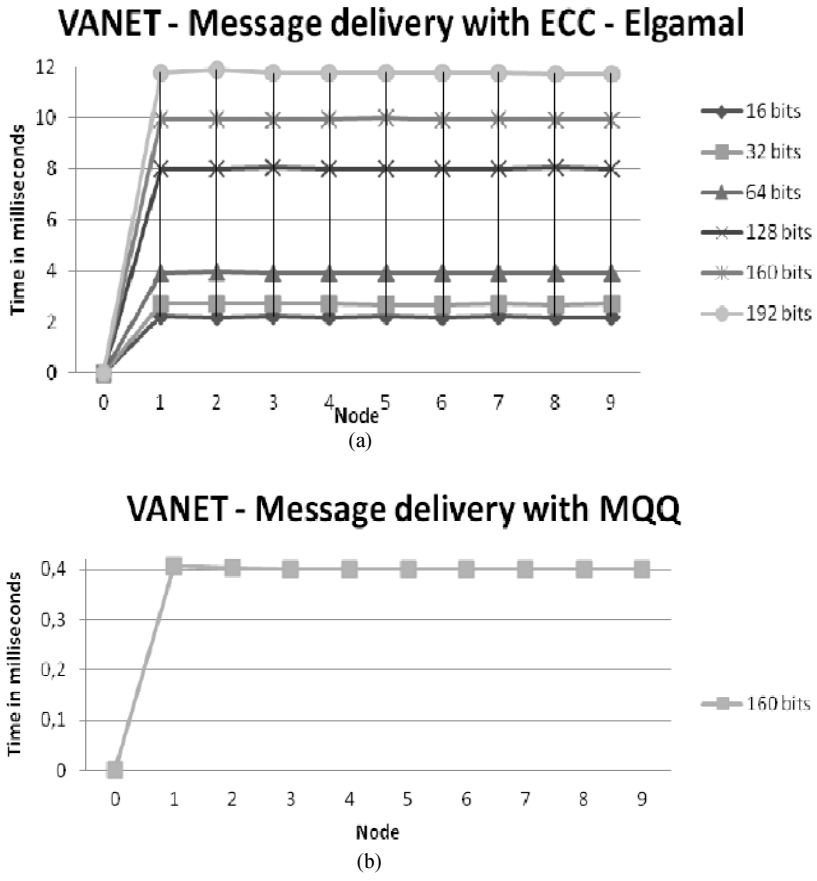


Fig. 5. Time of a communication in Vanet with ECC and MQQ

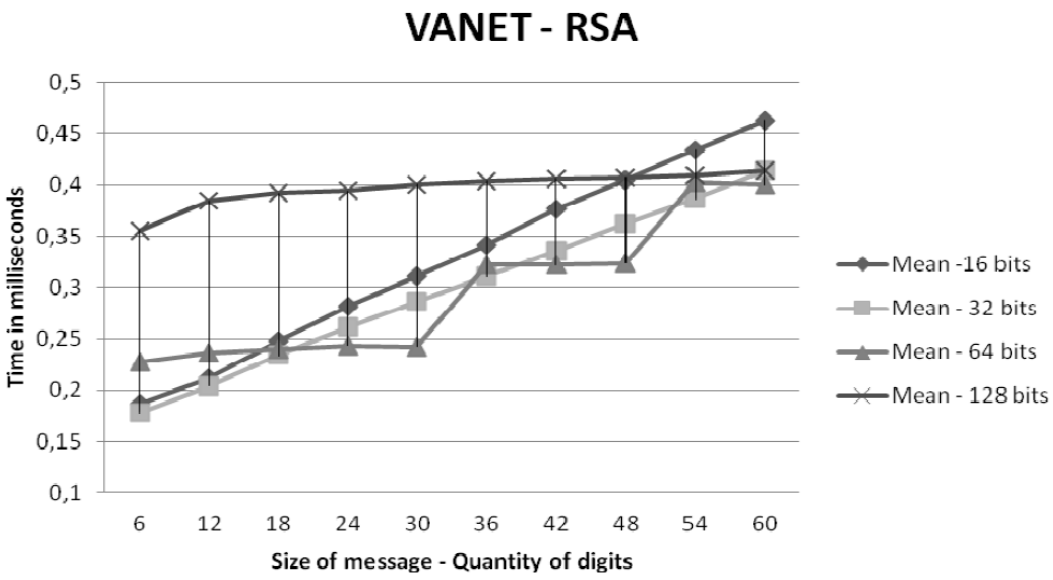
Again, we analyze the timing of a safe communication from all three algorithms, varying key size and message size that travels inside a VANET. Figure 6 shows the behavior of encrypted data deliver using the algorithm RSA.

When key size varies from 128 bits to 1024 bits, as it is shown by Fig. 6b, there is almost a time constraint of delivery, with a minimum variance, despite the quantity of digits that traveled, varying from 6 to 60. So, depending on the desired security level, it will practically have the same delivery time, despite the quantity of digits that travel inside a VANET. This is valid because communication happens with the messages considered small. It is

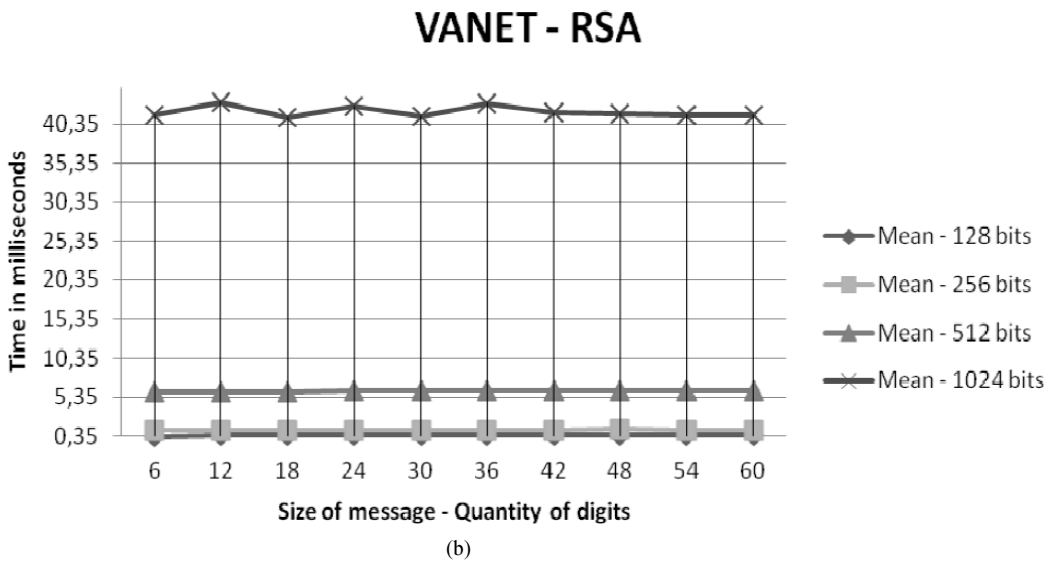
expected that raising the size of a message, communication time is also raised. Nevertheless, in this study we initially focus on short messages, once the initial goal was to verify the proper inclusion and behavior of these encryption algorithms in VANET scenarios.

Knowing that the minimum security level desired from the ECC algorithm is obtained by utilizing a 160-bit key, at least, Fig. 7a shows the increasing line of communication time, over the quantity of digits that travelled which, in this example, oscillates over 9 to 12 milliseconds. As security becomes bigger with bigger keys, we suggest using the ECC-ElGamal with a standard key of 192 bits, which offers a better security, as well as good runtime.

With MQQ algorithm, the key size compatible to the others is 160 bits, so, as expected, it is observed in Fig. 7b a growing curve when quantity of data that travels in the VANET increases. Yet, analyzing this graph, the difference of delivery time between one message of 06 digits and another one of 60 digits is 60 microseconds, with a proved effectiveness in terms of security, proportional to the size of the encrypted message of a 1024-bit RSA.

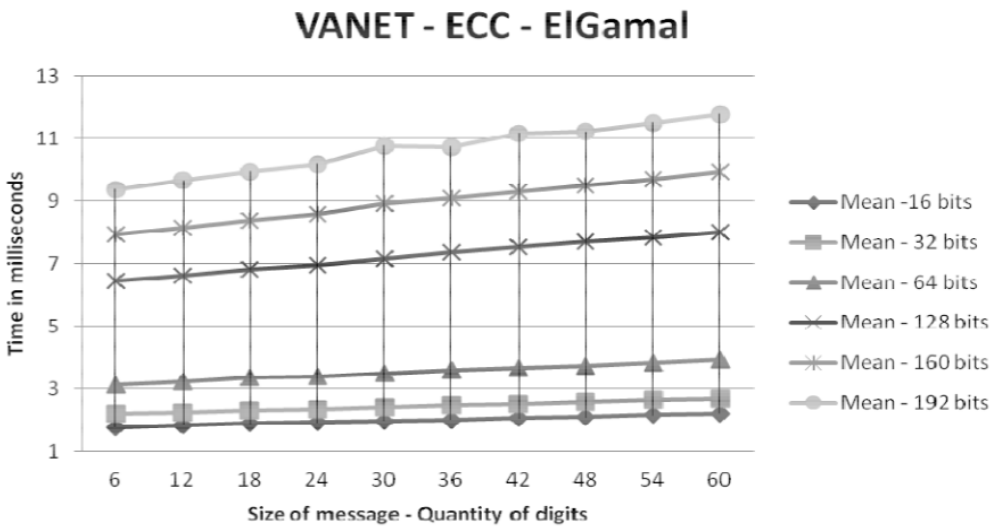


(a)

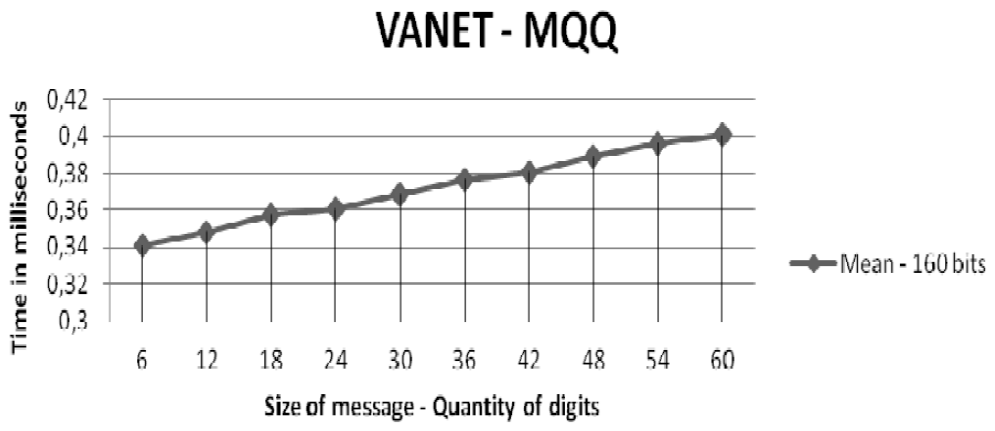


(b)

Fig. 6. Mean time using RSA, (a) keys to 128 (b) from 128 to 1K



(a)



(b)

Fig. 7. Execution time using ECC and MQQ

In the Fig. 8, a comparison of delivery time is made, using the algorithms as basis, with its compatible keys, for instance, 1024-bit RSA, 192-bit ECC and 160-bit MQQ, given a 30 digits message. Analyzing this result, it is possible to clearly realize MQQ efficiency, against other algorithms. While 1024-bit RSA has, on average, 40 ms of a safe communication, 192-bit ECC performs de same delivery on an average value of 10 ms and clearly with the 160-bit MQQ, it is possible to say that the delivery of the encrypted message is almost immediate. Despite MQQ performance values, it is necessary to examine the real security level offered by that algorithm. Therefore, MQQ shows a great potential, in terms of runtime, allowing a safe and fast communication.

As a result, we show in this study that aggregating security level, with an adequate runtime, to a VANET environment is doubtless a great alternative for safe communications for vehicular network applications, using asymmetric algorithms, which offer greater security once they allow, besides encrypting/decrypting, communication with reliability and authentication.

Thus, as shown in Fig. 8, the effectiveness of 160-bit MQQ algorithm for encrypted messages delivery, despite the quantity of digits this message has, we suggest MQQ as good alternative, besides the ECC, inside the service layer of protocol WAVE (IEEE 1609.2) and also, the ECC suggested by the protocol draft, if proof of its high performance is provided. Other point covered by this research is that, despite the algorithm compatibility of security level, it was perceived that depending on the size of the key used by the algorithm, in some cases, delivery times stood very close to each other. Hence, it is possible to have a VANET inside a encryption scheme with a lower security level, depending on the priority of the moment, in case it is delivery time of the encrypted message.

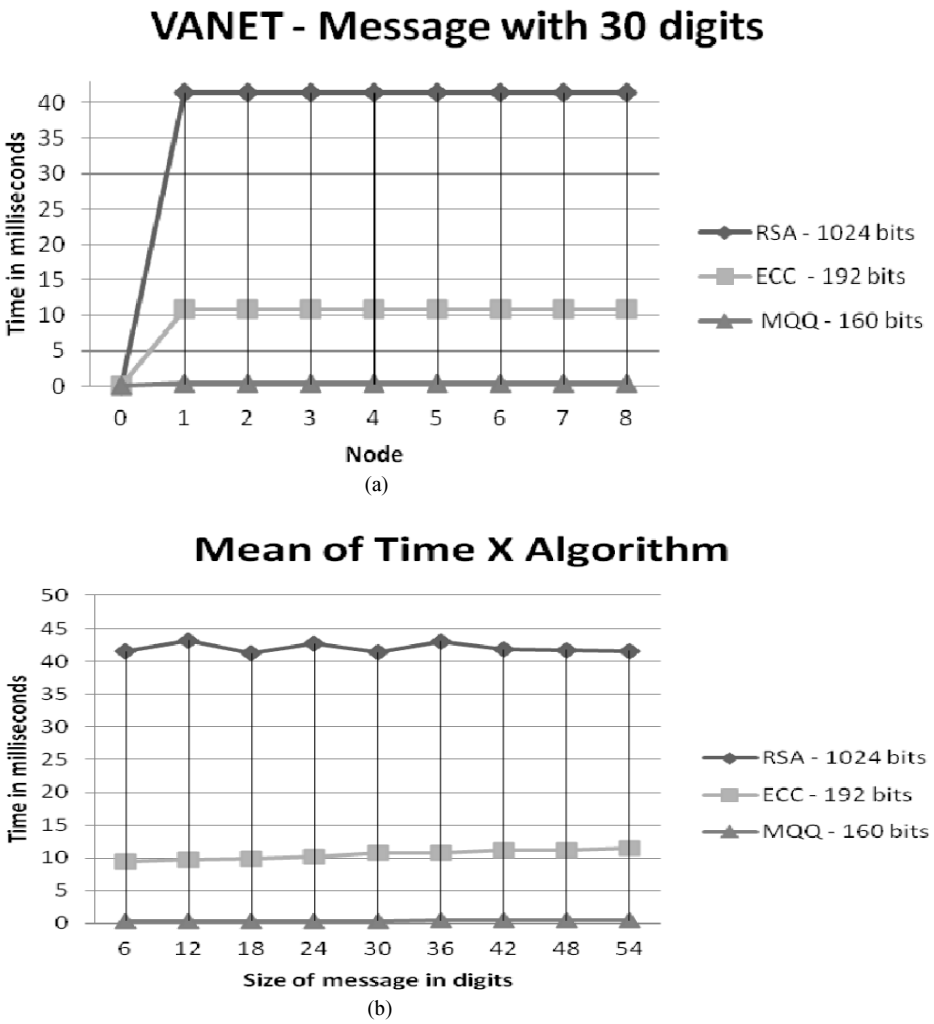


Fig. 8. Comparison of RSA, ECC and MQQ with compatible keys

In other words, if 160-bit MQQ or 192-bit ECC are not adopted, the 64-bit RSA can be used, because they are compatible by delivery time of encrypted messages. In this case, the compatibility point becomes delivery time instead of security level. After all, in a VANET, it is not necessary to have a compatibility of key size with a high security level, because the main characteristic of a VANET is the mobility of every node from the network, demanding speed on delivery and on encryption processes.

Related Works

Security in VANETS has been widely studied for many researchers, but the most of them do not present information about implementation or evaluation of symmetric or asymmetric algorithms working in a real environment of vehicular network. For this reason, in our knowledge, this paper presents worth study since it shows execution time of RSA, ECC and MQQ algorithms in different scenarios of Vanets. We use simulation, specifically, NS-3 and change the speed of nodes and insert communication among them using those asymmetric algorithms.

Choudhary (2007) investigated security aspects of vehicleto-vehicle communication using GPS and radar. Position is a key piece of information in vehicular ad-hoc networks (VANETs) and the use of radar will substantially augment the amount of trust that can be given to the received position information (Choudhary, 2007). The goal was to achieve local security by using onboard radar to detect neighbors and to confirm their announced GPS coordinates. They used preset position-based cells (through which we achieve local security) to create a communication network. Global security is achieved by exchanging packets among cell members and verifying neighboring vehicles' positions using oncoming traffic. Each vehicle generates information about the state of the traffic based on both what is seen

and what is received from other vehicles in the system. In this study asymmetric algorithms do not were considered neither inserted into the communication.

Abdalla *et al*. (2008) have provided an overview of the development of the communication standards and ongoing research for vehicular networks. Frequencies have already been allocated in North America and Japan and are expected soon in Europe. The IEEE 802.11p and WAVE suite were recently released for trial use. Routing protocols, broadcasting algorithms and security algorithms are being developed for vehicular networks as well as safety and commercial applications. Vehicular networks will not only provide safety and life saving applications, but they will become a powerful communication tool for their users. So, in this study (Abdalla *et al*., 2008) they reviewed the standardization work and researches related to vehicular networks and discussed the challenges facing future vehicular networks.

Ganesan *et al*. (2014) presented Temporary Anonymous Certified Keys (TACKs) as an efficient way to fulfill the security and privacy properties necessary for key management in VANETs. In TACKs, On-Board Units (OBUs) use short-lived keys to sign messages used for VANET communication. These short-lived keys are certified by Regional Authorities (RAs). During key updates, RAs verify that the requesting OBU is a legitimate OBU that has not been revoked; however, the RAs do not learn the OBU's identity. This allowed a valid OBU to acquire a certificate for a temporary key and preserve the OBU's privacy. It is very interesting solution for key management, as the authors conclude "Recipients need to authenticate OBUs that they communicate with; and road authorities would like to trace drivers that abuse the system. However, VANETs need to protect a driver's privacy. In particular, drivers may not wish to be tracked wherever they travel", but it does not present information about the impact of asymmetric algorithms.

Balasubramanian and Vijayalakshmi (2014) the authors presented a survey which describes the importance of security issues such as privacy at physical layer and the preserving scheme of privacy at mobile public hotspots in Nested NEMO based VANETs (NN-VANETs). This study focused with the security issues for MNN"s privacy and describes various techniques, to thwart the physical layer attack on the hotspots. So, the study discussion will bring the new idea about the privacy preservation and limitations of using such schemes on hotspots in Nested NEMO based VANETs, however there is nothing about evaluation of cryptography algorithms into the Vanet environment.

Shinde and Patil (2010) commented that vehicular networks will not only provide safety and life saving applications, but they will become a powerful communication tool for their users. In this study the authors provided an overview of the development of the communication standards and ongoing research for vehicular networks and added a section for security aspects. They conclude that a security system in VANETs must have the following features: Authentication, Data Integrity, Anonymity, Availability, Low Overhead, Privacy and Real-time Constraints. In this point, our paper analyzed asymmetric algorithms (RSA, ECC and MQQ algorithms) into real Vanet and we offer data and quantitative evaluation of these algorithms offering low overhead, data integrity, authentication and privacy and real time constraints.

Rajni and Singh (2013) the authors affirm the successful deployment of vehicular communication requires Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication with security to road safety and optimize road traffic. The technique used for secure communication in the presence of adversaries is known as cryptography. Cryptography refers to encryption in which a plaintext message is converted into a cipher text and this can be done with private-key or publickey. In this study, an algorithm based on private key encryption is used to make communication possible between two people with QualNet simulator. The algorithm used by authors reduces delay, increases throughput, provides authentication and higher security level in VANETs. The simulation carried from the help of QualNet Simulator and the length of Packet = 1024 Bytes. This paper is the most similar to our research work, since it effectively used and has implemented a cryptography algorithm. It used private algorithm explained by the authors, but it is not very known and used algorithm.

Al-Qutayri *et al*. (2010) the authors presented a study of VANETS. It highlighted their properties and security and privacy challenges such mobile *ad hoc* networks present. Furthermore, three main cryptography schemes were investigated: Public key, symmetric key and identity based cryptography, as they could be used for the security of the network. The advantages and disadvantages of these schemes were identified and overlapped with the properties of VAnets. Thus, this paper is in the same direction of our paper because it presented and explained the concepts of these schemes into VANET environment. We used, implemented and analyzed the impact of two (RSA and ECC) of the different mechanism mentioned in (Al-Qutayri *et al*., 2010).

Bhuvaneshwari *et al*. (2014) investigated VANET where the mobile nodes are vehicles that move on roads at very high speed following traffic rules; they provide communication between vehicle and vehicle (V2V) and Vehicle and Road side infrastructural unit (V2I). The authors (Bhuvaneshwari *et al*., 2014) proposed a new cluster model for efficient communication among the VANET nodes and created it along with security algorithms so that the communication among the VANET

nodes can be made in more efficient manner. They implemented and derived a set of encryption keys that are used to encrypt the next packet from part of the data in the current packet. The authors have showed the impact on the Throughput, Success ratio, Message delay, Handover traffic and Handover delay. Based on the described parameters simulation has been carried out using the Network Simulator (NS-2). In spite of this paper does not mention about what is the algorithm or scheme for generating the keys used into the encryption, it presented similar objectives and methodology as our paper, since we have used simulation and encryption mechanisms.

Singla and Sharma (2014) proposed solution designed to overcome these challenges like securely transmit data from sender to receiver by using Pretty Good Privacy (PGP) security and remove the traffic congestion or ignore the unnecessary load of network by selecting dynamic path for data transmission. In this, the hybrid protocol that is *Ad Hoc* On Demand Distance Vector (AODV) and Ad-Hoc on Demand Multipath Distance Vector (AOMDV) is used for to select the dynamic path in VANET. Central authority is provide the certificates to each node and verifies its certification. This proposed solution helps to increase the performance of network by making the accident free environment. It presented data about three metrics: Packet Data Ration comparison and End to End delay comparison and Average Throughput comparison, with and without PGP security and hybrid protocol. In spite of it has presented data and used a security model (PGP), the purpose and methodology is different from that used in our paper.

Agrawal *et al*. (2013) explained that communication between car to car, car to roadside unit are done through wireless communication. That is why security is an important concern area for vehicular network application. For authentication purpose so many bandwidth is consumed and the performance becomes low. In VANET some serious network attacks such as man in middle attack, masquerading is possible. In this study the authors compared various research papers on Vanet to analyze the current drawbacks and objectives in the Vanet research, but it does not propose or implemented any solution. The authors have mentioned in future they would like to propose an algorithm that would enhance the performance with the maintenances of security using a light weight mechanism.

Sakhreliya and Pandya (2014) used the MAC algorithm in the classical PKI system in place of ECDSA algorithm than it can reduce the processing overhead associated with ECDSA so time will be low for each message authentication and it also mitigate the problem of memory based and computation based DoS attacks that can be useful for the VANETs safety related applications as safety applications are time constraint. It has used the following parameters: Packet size is 232 and 262 bytes, Packet Interval 100-300 m and Transmission Range 250 m and used the NS simulator.

In these points, this paper presented results and conditions similar to ours. We used NS-3 and different scenarios, focused in packets varied up to 480 bytes and range interval inferior to 300 m. In the other side, the authors proposed the PKI-SC system that is Public Key Infrastructure (PKI) using Symmetric Key Cryptography (SC) in VANETs that use the symmetric key cryptography algorithm. They have told asymmetric key cryptography algorithms are more complex than, symmetric cryptography algorithm and takes more time. BUT, our results showed that asymmetric algorithms can be used for adding security in Vanets because there is overhead of this cryptography operations, but it is low and do not affect the communication in a relevant way among vehicles into the Vanets.

Vijayalakshmi *et al*. (2014), proposed a mechanism in order to provide secure and efficient communication in VANET environment. They overcome the drawbacks of the existing system by using Malicious Vehicular Analyzer algorithm and Elliptic Curve Cryptography (ECC). Using these algorithms, malicious messages are identified. It also detects the accident and other problems in the path of the vehicles. The ECC algorithm is used for stronger security during communication. Thus, it is similar to our proposed since we also have used the ECC algorithm and showed that it is possible to use in real Vanets scenarios, increasing the security into the communication.

Conclusion

This article presented a description of the impact symmetric algorithms can have on vehicular networks. More specifically, we succeeded to make an effective inclusion of the algorithms RSA, ECC and MQQ inside the VANET NS-3 simulator and we have shown results of how, in a simple scenario compounded of 10 to 50 nodes, which randomly varies speed between 60 and 100 km h^{-1}, located 300 m away from each other, it is possible to add security without affecting communication performance.

That is to say that there has been relevant contributions to scientific community, such as implementing security codes in a new simulator-the NS-3-, as well as having a proven analysis that besides using the ECC, as suggested by IEEE in the draft from 1609.2 standard, another possibility to utilize the MQQ, because his efficacy has been verified when compared with other algorithms studied.

As future works, we intend to explore more the existing resources in NS-3, create other scenarios that are closer to reality and also create topics for performance evaluating, varying speeds, distances, different routes, traffic engineering criteria and etc. Still on NS-3, we

expect understand how wi-fi 802.11p technology operates, how message discard is done and aggregate more security solutions.

Acknowledgement

This work was supported by CAPES, CNPq and FAPITEC/SE, Brazilian government Institutions for granting Science and Technology projects.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Abdalla, G.M.T., M.A. Abu-Rgheff and S.M. Senouci, 2008. Current trends in vehicular *Ad Hoc* networks. Ubiquitous Comput. Commun. J.

Agrawal, A., A. Garg, N. Chaudhiri, S. Gupta and D. Pandey *et al*., 2013. Security on Vehicular *Ad Hoc* Networks (VANET): A review paper. Int. J. Emerging Technol. Adv. Eng., 3: 231-235.

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

Al-Qutayri, M., C. Yeun and F. Al-Hawi, 2010. Security and privacy of intelligent VANETS. 1st Edn., INTECH Open Access Publisher, ISBN-10: 9537619281, pp: 29.

Amin, F., A.H. Jahangir and H. Rasifard, 2008. Analysis of public-key cryptography for wireless sensor networks security. WASET, 31: 530-535.

Balasubramanian, C. and G. Vijayalakshmi, 2014. Survey on privacy preserving scheme for hotspots in VANETs. Int. J. Innovative Res. Sci. Eng. Technol., 3: 804-808.

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.

Blake, I., G. Seroussi and N. Smart, 1999. Elliptic Curves in Cryptography. 1st Edn., Cambridge University Press, Cambridge, ISBN-10: 0521653746, pp: 204.

Branovic, I., R. Giorgi and E. Martinelli, 2004. A workload characterization of elliptic curve cryptography methods in embedded environments. ACM Comput. Architecture News, 32: 27-34. DOI: 10.1145/1024295.1024299

C2C, 2011. CAR 2 CAR communication consortium.

Chatterjee, K., A. De and D. Gupta, 2011. Software implementation of curve based cryptography for constrained devices. Int. J. Comput. Applic., 24: 18-23. DOI: 10.5120/2942-3914

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

El-Hadedy, M., D. Gligoroski and S.J. Knapskog, 2008. High performance implementation of a public key block cipher-MQQ, for FPGA Platforms. Sci. Technol.

Ganesan, B., B. Prabha and G.M. Sundari, 2014. An efficient privacy preserving scheme for VANET. Int. J. Comput. Sci. Mobile Comput., 3: 1342-1345.

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

Hankerson, D., S. Vanstone and A. Menezes, 2004. Guide to Elliptic Curve Cryptography. 1st Edn., Springer Science and Business Media, New York, ISBN-10: 038795273X, pp: 312.

ITS, 2011. Intelligent transportation systems standards fact sheet.

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209. DOI: 10.1090/S0025-5718-1987-0866109-5

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

Martinez, F.J., C.K. Toh, J.C. Cano, C.T. Calafate and P. Manzoni, 2009. A survey and comparative study of simulators for vehicular *ad hoc* networks (VANETs). Wireless Commun. Mobile Comput., 11: 813-828. DOI: 10.1002/wcm.859

Miller, V., 1986. Use of Elliptic Curves in Cryptography. SPRINGER, Advances in Cryptology-CRYPTO85 Proceedings, Williams, H.C., Springer, pp: 417-426. DOI: 10.1007/3-540-39799-X_31

Miracl, 2012. Multiprecision integer and rational arithmetic cryptographic library.

NS3, 2012. Ns-3 tutorial.

NS3hm, 2012. Ns-3-highway-mobility.

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

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

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

Rita, 2011. The Research and Innovative Technology Administration (RITA) coordinates the U.S. Department of Transportation's.

Rivest, R., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21: 120-126. DOI: 10.1145/359340.359342

Sakhreliya, S. and N. Pandya, 2014. Public Key Infrastructure (PKI) using Symmetric Key Cryptography (SC) in VANETs. Int. J. Comput. Sci. Inform. Technol., 5: 3556-3561.

Shinde, S.S. and S.P. Patil, 2010. Various issues in vehicular *Ad hoc* networks: A survey. Int. J. Comput. Sci. Commun., 1: 399-403.

Singla, R. and N. Sharma, 2014. Dynamic path selection with hybrid protocol and secure data transmission with PGP security in VANET. Int. J. Adv. Res. Comput. Eng. Technol., 3: 3827-3831.

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.

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

Vijayalakshmi, V., S. Saranya, M. Sathya and C. Selvaroopini, 2014. A Novel Mechanism for Secure and Efficient VANET communication. Int. J. Comput. Trends Technol.

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