Design a Cloud Security Model in VANET Communication: Implementation, Performance and Security Analysis

Hatem M. Hamad
Department of Computer Engineering
Islamic University of Gaza
Palestine, Gaza Strip

Alaaeddin B. AlQazzaz
Department of Computer Engineering
Islamic University of Gaza
Palestine, Gaza Strip

ABSTRACT

In the first paper of this work, the design and the architecture of our proposed model framework, VANET Security as a Service (VSaaS), was discussed. In this second paper, the performance metrics measurements will be investigated through the NS2, SUMO and Trans simulations, to evaluate the security overhead of the secure Vehicle Information Messages (VIMs), which are sent by the vehicles to the cloud as a coarse-grained information. Moreover, our proposed model framework (VSaaS) will be discussed against the security requirements in the VANET.

Keywords

VANET, Cloud, VSaaS, Certified Authority, Cryptography, Vehicle Information Messages, Traffic Information Messages, Authentication, Privacy, Security Overhead

1. INTRODUCTION

As shown in the first paper of this work, VANET Security as a Service (VSaaS) is a VANET security model, modular and hosted on a cloud. The VSaaS manages the security services and provides a secure VANET communication between the different entities e.g. vehicles, authorities and etc. The VSaaS proposal provided the following:

- VANET depends on cellular networks which acts as a gateway to the cloud to get services as the security services.
- VSaaS is responsible for:
  - Vehicles and authorities registration.
  - Key Management mechanisms to generate the keys for the different entities and renew the keys when they become expired.
  - Authenticating vehicles and their information messages. In addition to authenticating the authorities that interacting with the VSaaS.
  - Vehicle identity identification mechanism to preserve the privacy and enable the traceability only for the trusted authorities that have a permission to track the vehicles.
  - Providing security access list to manage the permissions between the different entities.
  - Providing a mechanism to revoke the misbehaved vehicle and the compromised authority.
  - Providing modules to process the secure Vehicle Information Messages (VIMs), which are sent by the vehicles as coarse-information messages, and construct fine-information messages, which called Traffic Information Messages (TIMs), that are disseminated to the vehicles based on their locations.

In order to show the feasibility of the VSaaS, the performance metrics measurements will be investigated in this paper through the NS2, SUMO and the Trans simulations, to evaluate the security overhead of the secure Vehicle Information Messages (VIMs), which are sent by the vehicles to the cloud as a coarse-grained information. Moreover, our proposed model framework (VSaaS) will be discussed against the security requirements in the VANET.

The rest of this paper is organized as: Section 2 presents the performance analysis of the secure Vehicle Information Messages (VIMs) in our proposed VSaaS. Section 3 presents the simulation results. Section 4 presents the security analysis. Finally, section 5 concludes the paper.

2. THE PERFORMANCE ANALYSIS OF THE SECURE VEHICLE INFORMATION MESSAGES (VIMs) IN OUR PROPOSED VSaaS

This section evaluates and analyzes the performance of the secure Vehicle Information Messages (VIMs), which are sent by the vehicles to the Certified Authority (CA) then to the storage where these components are hosted on the cloud. For a secure communication in the VANET, the security requirements should be satisfied. Therefore, there is a need to ensure that our proposed messages "Vehicle Information Messages (VIMs)" are effective and reliable. As a part of the security requirements, it is essential to meet certain performance requirements which guarantees that the VANET will work its function without any fail. Thus, the impact of the security model or protocols will be analyzed. In our work, the main security service is the (CA) which is responsible for the cryptographic and the authentication of the Vehicle Information Messages (VIMs), which are sent by the vehicles. The existing of the CA reveals two additional factors that should be taken into consideration, which are: the security overhead in the message size and the time taken for the encryption/decryption operations. As a result [1]:-

Secure VIM size = standard VANET safety message size + security overhead size (1)

Time Overhead = Encryption Time + Transmitting Time (delay) + Decryption Time (2)

2.1 Performance Matrices

This work investigates the throughput, end to end delay and the message delivery rate as in [2], [3] and [4], to evaluate the performance of our security model (VSaaS) against the Vehicle Information Messages (VIMs), and answer the important question: Is the public key cryptography (CA service) fit?

1. Throughput

Throughput is the number of the packets passing through the network during a certain time. It counts the total number of packets that have been successfully delivered to the desired node. The throughput increases as the node density increases. It is measured in bits per second (bit/s or bps). Throughput can be represented mathematically as in the equation below:

$$\text{Throughput} = \frac{no.of\ delivered\ packet * packet\ size * 8}{total\ simulation\ time} \quad (3)$$

2. End-to-End Delay

End-to-end delay is defined as the time taken for a packet to be transmitted across a network from the source to the destination. It is calculated by taking the average time for the data packet that arrive to the destination. It also includes the delay caused by the route discovery process and the queue in the data packet transmission. Only the data packets that are successfully delivered to the destination are counted. Furthermore, if the value of the delay is low, it means that the performance of the protocol is better. It is measured in second. The following equation is used to calculate the average end-to-end delay,

$$\mathrm{T_{E2E}} = \frac{\Sigma(T\_R - T\_S)}{n} \qquad (4)$$

$\mathrm{T_{E2E}}$is the average End-to-End Delay, T_R is the time of received packets at the destination node, T_S is the time of sent packets from the source node, and n is the number of nodes.

3. Message Delivery Rate

Message delivery rate is the sum of the successful received messages by all the nodes in the network per second. It is measured in messages per second. The following equation

is used to calculate the message delivery rate,

$$\text{Message Delivery Rate} = \frac{no.of\ delivered\ packet}{total\ simulation\ time} \qquad (5)$$

2.2 Simulation Setup

Our simulation work considers vehicles moving in a part of Cologne city which has a region size of 12594m x 6208m as shown in figure 1. This area has been covered by appropriate number of gateways that linked the vehicles to the cloud, where the CA and the storage are hosted. The simulation time has been set to 300 seconds. The Maximum Transmission Unit (MTU) has been set to 1500 bytes. The cloud delay was taken into consideration, which is approximately 30 milliseconds as mentioned in [5]. And, the cloud backbone bandwidth has been set to 100 Mbps. The mobility model of the vehicles includes the speed, accelerator and the positions, which are retrieved from the map using the SUMO and the Trans simulators. Moreover, ns2 was configured to support the roaming among the gateways.

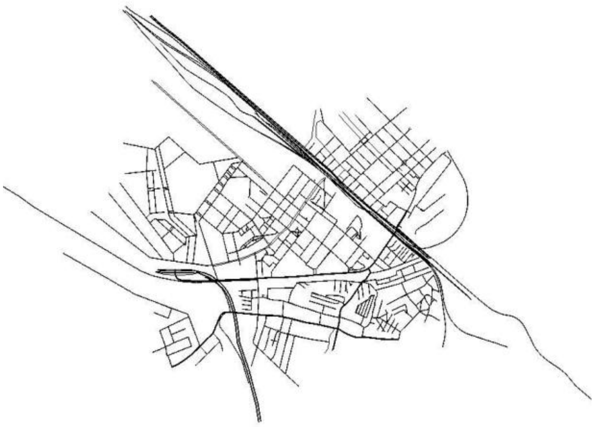

Figure 1: a part of Cologne city map

The aim of this simulation work is to evaluate the performance of our security framework model (VSaaS) against the secure Vehicle Information Messages (VIMs), which are sent by the vehicles to the CA, then to the storage where the CA and the storage are hosted in the cloud, as shown in the sample figure 2. And answer the important question: Is the public key cryptography (CA service) fit? To evaluate this security overhead, the performance metrics measurements should investigated.

Because of the existing of the CA, its overhead factors should be taken into the consideration, which are: the security overhead in the message size, and the time taken for the encryption/decryption operations.

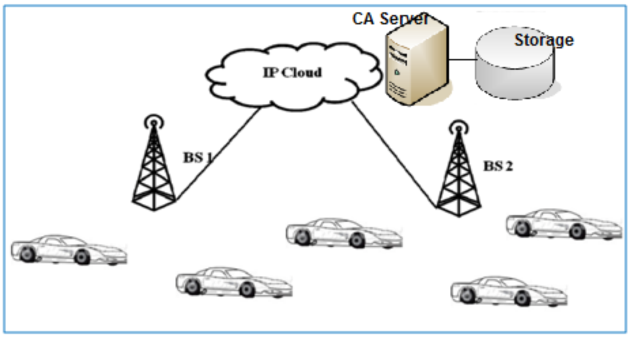

Figure 2: Sample Figure of Simulated Topology

2.3 The size overhead

The normal size of the Vehicle Information Messages (VIMs) has been set to 200 bytes including the header, timestamp, message type (MT) value and etc, and according to the standard, the typical size of the safety messages in the VANET is between 100 and 200 bytes without the security size overhead [6][7]. Where the security overhead in the message size of the secure VIMs is resulted because of the encryption operation, which has been done by using the CA's public key (we choose RSA-2048bit which expands the normal message by 56 byte). So, the size of our proposed secure message (VIM) becomes 256 bytes as described in the equation (1).

2.4 Benchmarks

The simulation of our proposed protocol needs to use a speed (time) benchmark for the selected cryptographic algorithms. In [8], many cryptographic algorithms are tested on three different machines:

1. Intel Pentium 4 (Prescott) processor. Algorithms are coded in C++ and compiled with MS Visual C++ 2005 SP1. The operating system is Windows Vista 32-bit.

2. Intel Core 2 1.83 GHz processor. Only one core of the CPU was used. Algorithms are coded in C++ and compiled with MS Visual C++ 2005 SP1. The operating system is Windows Vista 32-bit.

3. AMD Opteron 8354 2.2 GHz processor. Algorithms are coded in C++ and compiled with GCC 4.1.2. The operating system is Linux.

Table 1 shows the time needed by RSA2048 for the encryption and decryption operations on the selected machines.

Table 1: RSA-2048 Results

Millisecond/Operation	Mach. 1	Mach. 2	Mach. 3
RSA 2048 Encryption	0.22	0.16	0.08
RSA 2048 Decryption	10.53	6.08	2.90

2.5 Simulation scenarios

Scenario 1, the Simulation is executed for different number of vehicles: 25, 50, 75, 100, 125 and 150 with a normal message size of 200 bytes (without security), where the message rate is 0.3 second. Moreover, the simulation is executed again for different number of vehicles: 25, 50, 75, 100, 125 and 150 with security overhead (CA effects) where the message size becomes 256 bytes and take into consideration the encryption/decryption time overhead, and the message rate is also 0.3 second

Scenario 2, the Simulation is executed for fixed number of vehicles which is 50 vehicles with a normal message size of 200 bytes (without security) where the message rate is varied: 0.1, 0.2. 0.3, 0.4, 0.5 and 0.6 second. Moreover, the simulation is executed again for fixed number of vehicles which is 50 vehicles with security overhead (CA effects), where the message size becomes 256 bytes, and take into consideration the encryption/decryption time overhead, also the message rate is varied: 0.1, 0.2. 0.3, 0.4, 0.5 and 0.6 second.

3. SIMULATION RESULTS

3.1 Throughput Computation Cost

Throughput is the main measurement in the performance matrices. Therefore, some computational works should be made in order to inform us if the security overhead is acceptable or not before the starting with the simulation implementation. The using of the CA (Public key cryptographic) is proposed to support the security in the VANET, it is important to accept its overhead in the vehicular context. Theoretically, according to the numerical upper bounds, the throughput can be calculated by using the following equation [1]:

$$\text{Throughput } (kbps) = \frac{N\,x\,R\,x\,M\,X\,8}{1024} \qquad (6)$$

N is the number of vehicles, R is the messaging rate (message per second per vehicle) and M is the total message size (bytes).

Table 2 gives us the theoretical calculated throughput values from equation 6 for the secure VIM, when its size is 256 bytes, the message rate is 0.3 second and the number of vehicles is varied 25, 50, 75, 100, 125 and 150

Table 2: No. of vehicles vs. throughput for secure VIM

No. of vehicles	25	50	75	100	125	150
Throughput (kbps)	162.5	325	487.5	650	812.5	975

And, Table 3 gives us the theoretical calculated throughput values from equation 6 for the secure VIM when its size is 256 bytes, the number of vehicles is 50 vehicles and the message rate is varied 0.1,0.2, 0.3, 0.4, 0.5 and 0.6 second.

Table 3: Message Rate vs. throughput for secure VIM

Message Rate (sec)	0.1	0.2	0.3	0.4	0.5	0.6
Throughput (kbps)	977	488	325	244	195	163

In the tables 2 and 3, the results show to us that the throughput increases linearly with the increase in the number of the vehicles, and with the increase in the message rate. All the throughput values are below 1 Mbps, which are afforded by the cloud-based infrastructure. Thus, as far as throughput is concerned and the effect of CA is acceptable. Moreover, the simulation results should be as similar or less than those calculated values.

3.2 Simulation Results: Scenario 1

1. Throughput

Figure 3 shows the system throughput of the normal messages and the secure messages sent by the vehicles. Normally, the throughput increases linearly with the increase in the number of the vehicles, because the increasing in vehicles' number increases the number of the sent packets, which is resulted in the increasing number of the delivered packets. The delivered packets is the main factor in the throughput equation (3).

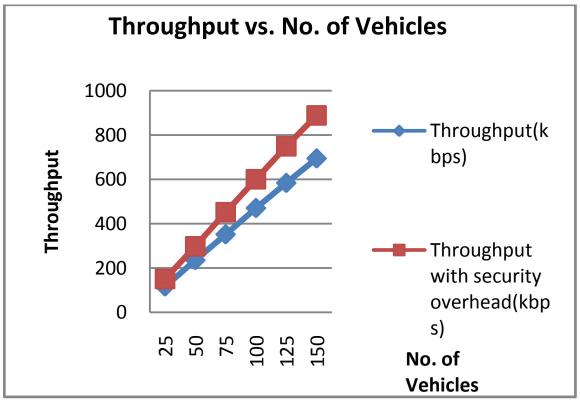

Figure 3: Throughput vs. No. of Vehicles for both normal and secure messages

Also, the effect of the CA in the throughput is shown in the figure 3, the throughput of the secure messages is more than the throughput of the normal messages, according to the security overhead in the message size that increases the throughput. But, this effect is acceptable because the infrastructure's throughput capacity can afford this overhead, and as shown in figure 3, the throughput did not exceed 1 Mbps, even when the 150 vehicles sent secure messages to the CA at the same time.

Finally, the throughput values of the simulation results are agreed with the computational works in table 2, because all the throughput values which got from the simulation are below the numerical upper bounds.

2. End-to-end delay

Figure 4 shows the end-to-end delay of the normal and secure messages sent by the vehicles. That delay is not be considered when the number of the vehicles increases, because of the low contention on the medium.

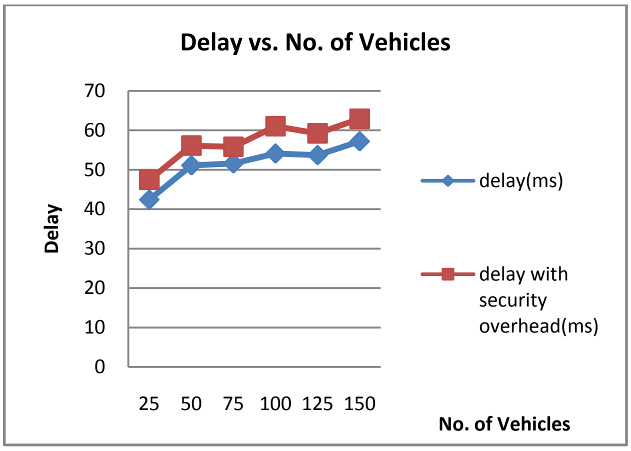

Figure 4: Delay vs. No. of Vehicles for both normal and secure messages

Also, there is no considerable effects of the CA in the delay as shown in the figure 4. This is because the infrastructure can afford the security overhead in the message size and the cryptographic operations time overhead, according to the low contention on the medium and the high transmission rate that minimizes the effects of security overheads. Thus, the CA and the cryptographic operations do not critically affect the delay.

In addition to, the delay values are between 42 ms and 63 ms; which are acceptable and good results in the cloud environment.

3. Message delivery rate

Figure 5 shows the message delivery rate of the normal messages and the secure messages sent by vehicles. Normally, the message delivery rate increases linearly as the number of vehicles increases, because the increase in the vehicles' number increases the number of the sent packets, which is resulted in the increasing number of the delivered packets. The delivered packets is the main factor in the message delivery rate equation (5).

Also, there is no considerable effects of the CA in the message delivery rate as shown in the figure 5. This is because the infrastructure can afford the security overhead according to the low contention on the medium and the high transmission rate that minimizes the effects of the security overhead in the message size. Thus, the CA and the cryptographic operations do not critically affect the message delivery rate.

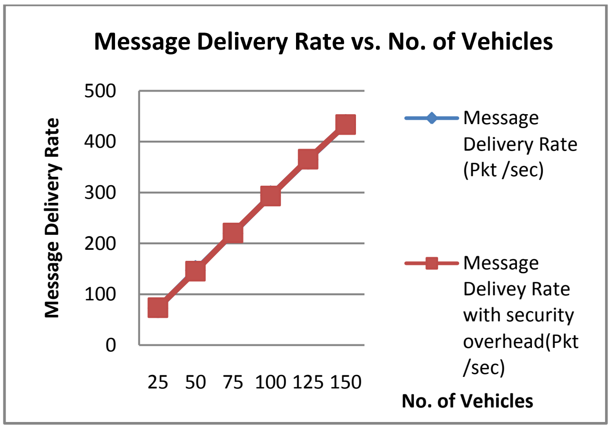

Figure 5: Message delivery rate vs. No. of Vehicles for both normal and secure messages

3.3 Simulation Results: Scenario 2

1. Throughput

Figure 6 shows the system throughput of the normal messages and the secure messages sent by the vehicles. Normally, the throughput decreases as the message rate value increases, because the increasing in the message rate value means decreasing in the number of the sent packet per second, which is resulted in the decreasing number of the delivered packets. The delivered packets is the main factor in the throughput equation (3).

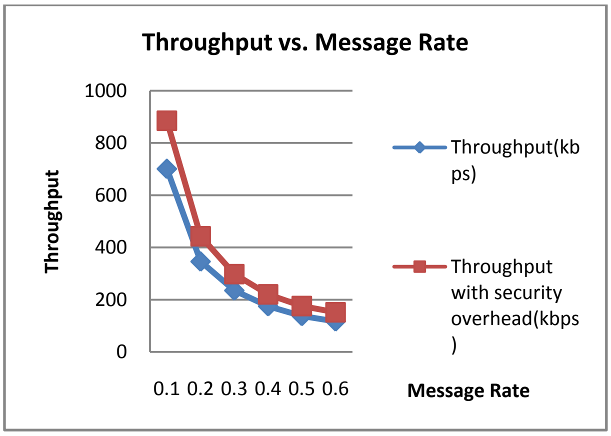

Figure 6: Throughput vs. Message Rate for both normal and secure messages

Also, the effect of the CA in the throughput is shown in the figure 6, the throughput of the secure messages is more than the throughput of the normal messages, according to the security overhead which increases the message size that increases the throughput. But, this effect is acceptable because the infrastructure's throughput capacity can afford this overhead. And as shown in figure 6, the throughput does not exceed 1 Mbps, even when the message rate of the secure message is set to maximum (10 messages/vehicle/second).

Finally, the throughput values of the simulation results are agreed with the computational works in table 3, because all the throughput values which got from the simulation are below the numerical upper bounds.

2. End-to-end delay

Figure 7 shows the end-to-end delay of the normal messages and the secure messages sent by vehicles. That delay is not be considered when the message rate varied from 0.1 to 0.6 seconds, because the infrastructure can afford this variation for both normal and secure messages according to the low contention on the medium and the high transmission rate that minimizes the effects of the variation in the message rate.

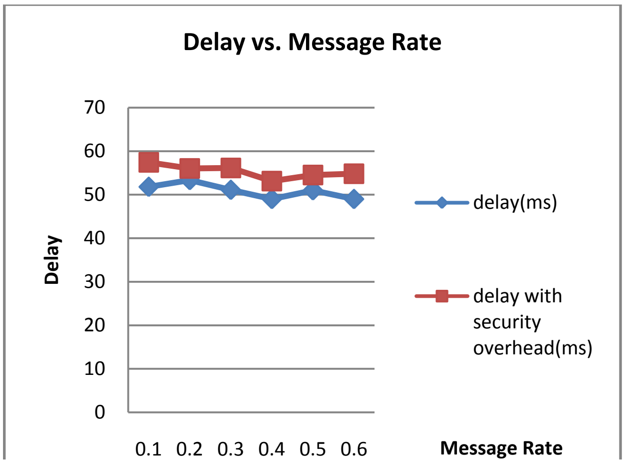

Figure 7: Delay vs. Message Rate for both normal and secure messages

Also, there is no considerable effects of the CA in the delay as shown in the figure 7. This is because the infrastructure can afford the security overhead in the message size and the cryptographic operations time overhead according to the low contention on the medium and the high transmission rate, that minimizes the effects of these security overheads. Thus, the CA and the cryptographic operations do not critically affect the delay.

In addition to, the delay values are between 49 ms and 57 ms, which are acceptable and good results in the cloud environment.

3. Message delivery rate

Figure 8 shows the message delivery rate of the normal messages and the secure messages sent by the vehicles. Normally, the message delivery rate decreases as the message rate value increases, because the increase in the message rate value means a decrease in the number of the sent packet, which is resulted in the decreasing number of the delivered packets. The delivered packets is the main factor in the message delivery rate equation (5).

Also, there is no considerable effects of the CA in the message delivery rate as shown in the figure 8. This is because the infrastructure can afford the security overhead according to the low contention on the medium and the high transmission rate that minimizes the effects of the security overhead in the message size. Thus, the CA and the cryptographic operations do not critically affect the message delivery rate.

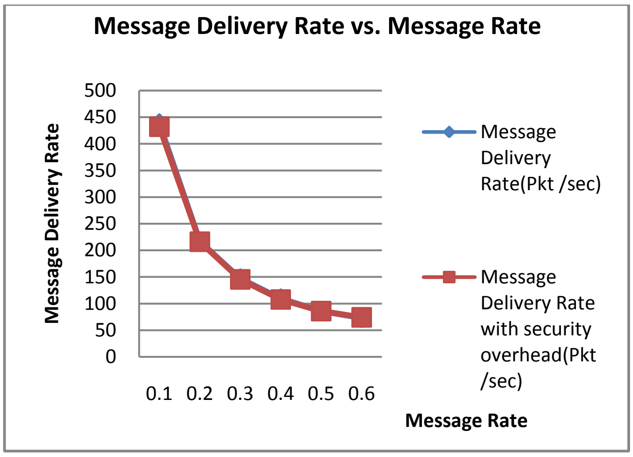

Figure 8: Message delivery rate vs. Message Rate for both normal and secure messages

4. SECURITY ANALYSIS

Firstly, our proposed model framework (VSaaS) will be discussed against the security requirements in the VANET. After that, some related security issues also will be discussed.

4.1 VSaaS Against Security Requirements in VANET

1. **Identification and Authentication**: the CA, which is a part of the VSaaS model, generates an identifier to every vehicle, which is called Vehicle Identification Number (VID), before giving a license to the work and registers this VID with CA itself. Thus, it should be understood that, the CA can identity and verify the vehicle by its VID to determine if it is a legitimate vehicle or not, where this VID should be added to the vehicles' messages in a secure way. This Identification prevents the intruders from sending false messages. It is not possible to track the VID of the vehicle only through the authorities that have a traceable permission. Also, CA generates an identifier to every authority, which is called Authority Identification Number (AID). Thus, it should be understood that, the CA can identity and verify an authority by its AID, to determine if it is a legitimate authority or not. This Identification prevents the intruders from cooperating with the VSaaS model.

2. **Privacy and Anonymity**: For liability, vehicles' identities (VIDs) should be added to the vehicles' messages, but this requirement contradicts with the privacy. Therefore, vehicles' identities should be hidden (encrypted) from the others, only the CA can identify the vehicles' identities. To solve it, the CA generates a symmetric key which is called the privacy key K_{priv}, it is used to encrypt/decrypt the vehicles' identities (VIDs). The VID is concatenating with the current reading (xy-coordinates) which is taken from the tamper GPS, then encrypting the all with the privacy key K_{priv} to produce the EVID, which is added to each message as an alternative of the clear VID. It is worth to mention that, the privacy key K_{priv} provides authentication and privacy. Authentication is achieved because only the registered and trusted vehicles have this privacy key K_{priv}, where it is used to encrypt/decrypt the vehicles' identities (VIDs). Using the same privacy key K_{priv} by all the vehicles at the same time, provides anonymity which achieves the privacy. And, the concatenating xy-coordinates to the VID every time

before encryption, ensures that the EVID value is different for every message, and mitigates the linking between the two messages generated from the same vehicle. Also, the EVID is a part of the vehicles' messages, where the whole message is encrypted by the CA's public key. Thus, only CA can decrypt the whole message by the CA's private key to get the EVID.

3. **Confidentiality:** all the messages sent by the vehicles and authorities are encrypted by the CA's public key. Thus, only CA can decrypt the messages by the CA's private key. In addition, the CA generates the secret shared key K_{SM} that will be used to exchange the information and messages between the authority and the VSaaS modules. This keeps the content of messages secret.

4. **Authorization:** the VSaaS provides the authorization through proposing a security access list (ACL), to manage the permissions. The ACL represents a set of permissions and rules to Allow/deny the inter-actions between the different entities (vehicles, authorities, VSaaS modules) and the intra-actions between the modules within the VSaaS. Our design of VSaaS is modular. It is easy to add new types of authorities, databases and VSaaS's modules by defining their permissions.

5. **Availability:** It is essential for the part of security availability to meet certain performance requirements, which guarantees the VANET will work its function probably without any fail. This work simulated and evaluated the secure Vehicle Information Messages (VIMs) with the security overhead (CA effects).The performance of the secure Vehicle Information Messages (VIMs) is acceptable. The impact of the security overhead appears in the throughput because the security overhead in the message size has an increasing in the throughput, but this effect is acceptable because the infrastructure's throughput capacity can afford this overhead. There is no considerable effects of the CA in the message delivery rate and end-to-end delay because the low contention on the medium and the high transmission rate, minimize the effects of the security overheads. But, the availability of system like that, is something that cannot be fully guaranteed. The primary vulnerability, which lies in the different types of wireless technologies, is considered as jamming attacks. Also, the DoS attacks can be realized by sending too many messages to the specific destination, therefore, there won't be enough time to process the valid messages. Detection and prevention of the DoS also require mechanisms, hardware and software to satisfy the concept of the intrusion detection and prevention.

6. **Non-Reputation:** Non-Repudiation is achieved in our work because of the following reasons: 1) The VSaaS is resistant against the masquerade attack. 2) Vehicles cannot cheat about their positions and related parameters because a secure positioning solution is used in the messages. 3) The vehicle cannot deny having a sent message, because it includes the vehicle's identity concatenated to its real xy coordination, and encrypts the all by the privacy key K_{priv}. 4) The vehicle cannot claim that the message was replayed because the timestamp is included in each message.

7. **Entity Revocation:** The VSaaS provides mechanisms to revoke the vehicles and authorities when they are engaged in a malicious activity. But, the methodology to determine a malicious activity is out of our scope work.

4.2 More in Security

Messages are provided by the timestamps to guarantee the message freshness and provide protection against the reply attacks. Only the authorities, that have a traceable permission, can track a vehicle through its VID.

All mentioned keys in the VSaaS framework model are changed frequently in a way to keep the content of messages secret, and prevent any attempts to uncover these keys. Moreover, the VSaaS provides mechanisms to change the keys if any compromising happens.

It is not possible to send a false location, because the algorithm of the sending secure VIM reads the (xy-coordinates) from the tamper GPS, which is build-in on the vehicles, and concatenates it to the VID in order to produce the EVID that is a part of the messages sent by the vehicles. Moreover, each vehicle has a tamper-proof device (TPD) installed by the manufacturer, to store all the secret information used in the VANET. It is fabricated such as no one can reveal or compromise its information. TPD should erase all the secret information if it is removed from the vehicle. This is providing a physical security to the TPD.

The integrity mechanisms do not mentioned to in our work because of the encrypting of the whole message was proposed. Thus, it is meaningless to take into consideration any integrity mechanisms with encrypting of the whole message. To send secure VIMs, a security level was assumed to be equivalent at least to RSA 2048, which is supposed to survive until 2030.

5. CONCLUSION

In this paper, the throughput, end-to-end delay and the message delivery rate was investigated through the NS2, SUMO and the Trans simulations, to evaluate the security overhead of the secure Vehicle Information Messages (VIMs). The impact of the security overhead appeared on the throughput because the security overhead in the message size has an increasing in the throughput, but this effect is acceptable because the infrastructure's throughput capacity can afford this overhead. There is no considerable effects of the CA in the message delivery rate and end-to-end delay, because the low contention on the medium and the high transmission rate minimizes the effects of the security overheads. Moreover, our proposed model framework (VSaaS) was discussed against the security requirements in VANET.

VSaaS model framework is secure, efficient, modular, managed by cloud, resistant against attacks and fulfills the security requirements.

6. REFERENCES

[1] M. Raya and J. P. Hubaux. The Security of Vehicular Ad Hoc Networks. In SASN ’05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pages 11–21, New York, NY, USA, 2005. ACM.

[2] V. Khairnar and K. Kotecha, Simulation-Based Performance Evaluation of Routing Protocols in Vehicular Ad-hoc Network. International Journal of Scientific and Research Publications. vol. 3, no. 10, October , 2013.

[3] Y. Khasa and Pooja, Performance Evaluation of Routing Protocols in MANET. International Journal of Computer

Science Engineering andTechnology (IJCSET). vol . 6, no. 3,p.p 109-112, March , 2016.

[4] P. Rohal, R. Dahiya and P. Dahiya, Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV), International Journal for Advance Research In Engineering And Technology (IJARET). vol. 1, no. 2, p.p 54-58 March. 2013.

[5] M. A. Al Mamun, K. Anam, M. F. Onik, A M Esfar- E-Alam, “Deployment of Cloud Computing into VANET to Create Ad Hoc Cloud Network Architecture”, Proceedings of the World Congress on Engineering and Computer Science, USA, 2012, vol. 1, ISBN 978-988-19251-6-9

[6] Q. Xu, T. Mak, J. Ko, and R. Sengupta. Vehicle-to-vehicle safety messaging in DSRC. In Proceedings of the first ACM workshop on Vehicular ad hoc networks, pages 19–28. ACM Press, 2004.

[7] X. Yang, J. Liu, F. Zhao, and N. Vaidya. A vehicle-to-vehicle communication protocol for cooperative collision warning. In First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2004), August 2004.

[8] Crypto++ 5.6.0 Benchmarks, http://www.cryptopp.com/benchmarks.html ,accessed Mar. 2012.