Improving Vehicular Authentication in VANET using Cryptography

Rasha Al-Mutiri[1], Mznah Al-Rodhaan[2], and Yuan Tian[3]

Department of Computer Science
King Saud University, Riyadh, Saudi Arabia

Abstract: In the last several years, many types of research are focusing on Vehicular Ad-hoc Networks (VANETs) field due to the lifesaving factor. VANETs are defined as a set of vehicles in the road interact with other vehicles or with the Road Side Unit (RSU) through wireless Local Area Network (WLAN) technologies. The fundamental advantages of VANETs are enhancing the road and driver's safety and improving the vehicle security against adversaries' attacks. Security is the most difficult issue belonging to VANETs since messages are exchanged through open wireless environments. Especially in the authentication process, the vehicles need to be authenticated before accessing or sending messages through the network. Any violation of the authentication process will open the whole network for the attack. In this paper, we applied security algorithms to improve authentication in VANETs with four stages of cryptography techniques: challenge-response authentication, digital signature, timestamping, and encryption/decryption respectively. Also, we also proposed an algorithm model and framework. Finally, we implemented the challenge-response authentication technique, and then measured and evaluated the result from the implementation.

***Keywords*:** VANETs, Security, Authentication, Cryptography, OMNET++.

1. Introduction

As the internet grows, Intelligent Transportation System (ITS) evolution has made a big leap, which helps to improve the safety of the roads, the condition of driving and reduce accidents [1][2]. Vehicular Ad-hoc Networks (VANETs) provide a solution for the drivers' safety and traffic problems [1]. Many researchers are focusing on different areas of VANETs such as routing, broadcasting, and security [3].

VANETs consist of vehicles that equipped with radio communication, as in Mobile Ad-hoc Networks (MANETs). The communication between vehicles is arranged in an ad-hoc manner with an IEEE 802.11g based Wi-Fi communications system, supported with a wireless roadside base station network [4]. VANETs are mainly used in reducing accidents, traffic jam and help in road intersections. Smart vehicles have a set of sensors to handle environmental information that are helpful for drivers, such as radar and Global Positioning System (GPS) [1]. Every vehicle in the network is acting as the host and the router to perform suitable functions [5]. VANET is a wireless network designed with various characteristics. Using wireless medium in VANET may cause some drawbacks that make the network defenseless to many types of attacks such as eavesdropping, denial of service, jamming, etc. [1].

There are many VANET security requirements, which need to be secure and satisfied, one of these requirements is the authentication process, which is a big challenge in VANET security due to the characteristics of the network. All the vehicles need to be authenticated before accessing the network; any violation of the authentication process will make the whole network vulnerable for the attack. Authentication protects the network from the insider or the outsider attacker that uses falsified identity [1, 2]. The significant of the authentication process comes from the fact that it is always used whenever a vehicle access or send messages in the network. There are many kinds of attacks affect the authentication process such as Sybil attack, spoofing attack, position faking the attack, etc. [1].

Various tools and techniques are used in VANET to prevent from security attacks. One of these techniques is cryptography, which considers one way to detect and solve security threats [1]. Cryptography has many methods such as encryption/decryption algorithms, hash functions, keys generation, digital signature, time-stamping and other techniques [1]. Many authors proposed solutions for the authentication process using cryptography and most of them suggested using secure hardware and digital signature to detect and prevent attacks.

Today, the roads are a dangerous place that is affected by traffic and accidents. According to al-Arabiya news website, published in 2013, Saudi Arabia is the first country worldwide in the number of accidents; there were 7,153 deaths from accidents in 2011 [6]. Most of these accidents caused by speed, cutting a red light, and lack of driver's attention [6]. Therefore, securing roads and helping the driver's focus is a fundamental obligation. It is important to satisfy driver's needs and give solutions to driver's safety and traffic problems [1].

Vehicular Ad-hoc Networks (VANETs) provide a solution for the driver's safety and traffic problems, but the question is what if the attacker gain accesses to the network, can he cause an accident? Like other networks, VANETs are vulnerable to many attacks that may danger the driver and passengers' life. Therefore, the security threats in VANETs need to be minimized to avoid safety violation in the network [1].

Authenticating the vehicles in the network is an important step because all vehicles use it whenever the vehicle accesses or sends messages in the network and it prevents the malicious attacks.

VANET safety is essential because it affects the driver's life. It is necessary to keep the exchange information in the network secure and protect it from the attackers. Besides, it is also important that all vehicles authenticate whenever it accesses or sends messages in the network, all information needs to be transmitted correctly and within time [7]. The VANET security is hard to implement because of the speed of vehicles and the size of the network [2]. The main objectives that will be achieved in this paper are finding a way to improve the security authentication in VANETs using cryptography to improve the driver's safety and

experience, and reduce the number of accidents. And making VANETs be more secure and trustworthy.

In this paper, we proposed an authentication algorithm to improve the authentication mechanism for VANETs using a combination of different cryptography techniques, which provide higher security [1]. Challenge-response authentication, digital signature, time-stamping, and encryption/decryption are used in the proposed algorithm, in which the keys are used whenever the vehicle starts its journey. The algorithm improves security, prevents attacks over the network and avoids the threats that may affect the driver's life.

Our paper organized as follows: Section 2 discusses the related work of VANET. Section 3 discusses the new authentication algorithm, discusses its model and framework and presents keys management protocol. Section 4 represents our contributions by this paper. In Section 5, we present the algorithm simulation and performance. The simulation results are discussed in Section 6. Finally, the conclusions, limitations, and potential future works are given in Section 7.

2. Related Work

VANET is a subclass of MANET, where nodes are considered as vehicles, and it has many properties that are different from MANETs [8, 9], such as vehicles' mobility, no fixed infrastructure, scalability and dynamic topologies. However, with these properties in VANETs the vehicles move in a predicted way because it is controlled by the road structure [8].

VANETs aim to enhance the safety of the roads, prevent accidents, comfort the passengers and help vehicles to communicate with other vehicles or roadside infrastructure [8-10]. The VANETs goal is to allow vehicles to communicate with each other [11]. For communication, each vehicle is equipped with short and medium range wireless communication so that it could transmit messages with other vehicles or with Road Side Units (RSUs) placed on the road [10-12].

VANETs can be categorized to safety and non-safety (user) applications [3]. The characteristic set of applications (e.g. accident warning and traffic management), resources (e.g. power source), and the environment (e.g. traffic flow patterns and infrastructure) make the VANETs different from other wireless communication [13].

One of the critical requirement in VANETs is the ability to exchange safety messages correctly and immediately with a low probability of losing or corrupting messages [8]. VANETs have several issues that need to be solved, such as security and bandwidth, which increases in traffic, intersections and buildings [8]. Implementing the security in VANETs is needed to provide a safe wireless environment, which leads to prevent attackers from attacking driver's life. Because if the attackers alter the message content, vehicles are affected immediately [14].

There are two possible ways for vehicles to communicate with each other, vehicle to vehicle (V2V) communication and vehicle to infrastructure (V2I) communication [8][9].

V2V communication: Offers interaction between vehicles, where vehicles can send and receive any messages, such as traffic conditions messages. It mostly suited for short-range vehicular communications [15].

V2I communication: Offers interaction between vehicle and infrastructure such as RSU, to share information such as road condition and speed limit [1, 2]. The communication is similar to a wireless link between the mobile node and access point [15]. In addition, there are two types of messages that can be exchanged regarding safety: safety and non-safety messages. Exchanging messages provide safety and make the drivers act fast in case of life threating events [10].

Safety messages: do not contain any confidential information but contain sensitive information that usually needs to broadcast as fast as possible by vehicle or RSU, [16] such as emergent braking, accident or traffic [13].

Non-safety or confidential messages: mostly contain confidential information and usually are sent privately to another vehicle, such as peer to peer communication.

Cryptography technique can be used in VANETs authentication, it can be done by various types of algorithms and protocols. Using a combination of different algorithms will provide a higher efficiency and stronger security compared to using individual protocols. [1] Below we mention few cryptography techniques that are widely used in VANET area:

- **Public Key Infrastructure (PKI)**

PKI is the most technique that is used in VANETs for user authentication [16]. It is related to the idea of asymmetric cryptography. The public key is shared with others and used to ensure no one can decrypt the message except the private key owner. While the private key is protected and used to ensure the identity of the user.

Certificate Authorities(CA) is an authority that issues certificates, sign the messages digitally and provides the private and public key to ensure the authentication of users [16][17]. In VANETs, we need a certified CA to deny any discrepancy, it can be from government authority or vehicle manufacturers, and there will be many CAs where each one is related to a region [17]

- **Digital Signatures**

Digital signature uses asymmetric authentication and is wildly used in VANETs. Asymmetric cryptography delays the delivery of safety messages. So, digital signature preferred to use because it delivers the messages quickly and its simplicity [16][17]. The vehicle sends messages after encrypting it using the receiver public key then digitally signs it. Public key cryptography affords data protection, while digital signature affords sender authentication. The receiver would know if the message altered because the digital signature would not be the same. Digital Signatures ensure the authentication of the user, message integrity, and non-repudiation.

- **Time Efficient Stream Loss-Tolerant Authentication (TESLA)**

TESLA used for multicast and broadcast communications [16][18]. Instead of using public and private key (Asymmetric Cryptography) it uses deferred key (Symmetric Cryptography). It implements a broadcast authentication, which is the same as unicast authentication [16].

The sent messages are stored in the receiver's memory until the deferred key uncovered. At the receiver side, storing junk messages may cause performance to suffer or system to

crash [16][18]. TESLA depends on time to authenticate the messages, granting only the sender to provide a broadcast authentication (key) after periods of time. This type of technique reduces the authentication overhead, but it does not provide repudiation service and opens the network to Denial of Service attacks [16][18].

- **TESLA++**

TESLA++ is better than TESLA in terms of efficiency, advance, and security. It the same as TESLA where uses symmetric cryptography and deferred key disclosure. The main advantage of TESLA++ is to reduce the receiver's memory and prevent DoS attacks [16]. The receiver does not need to store all the MAC, only the ones the receiver generated, MAC is broadcast at first then the message and the deferred keys. Unnecessary MACs are discarded from memory such as older MACs or message and its key [16].

- **Elliptic Curve Digital Signature Algorithm (ECDSA)**

ECDSA is mathematically derived from digital Signature. ECDSA is more secure and faster in distributing messages after the user authenticated. For user authentication, ECDSA needs less storage size and less response time [16]. It can be used to verify and produce signatures. Also, to provide user authentication, ECDSA uses the asymmetric key, it generates the public key by multiple a random number with the base point and generates the private key using an integer. [16] ECDSA is more reliable and secure, but it is vulnerable for two attacks, Elliptic Curve Discrete Logarithmic Problem (ECDLP) attack and hash function attack [16].

- **Challenge-Response Authentication**

Using the public key and digital signatures to authenticate safety messages has an issue, is that the attacker can flood the receiver by malicious safety message, which led to a delay in decoding the real safety message [16]. As a solution, the authors in [16] use challenge-response authentication technique.

In this technique, the receiver sends a challenge to the sender whenever he receives a message, the sender response to the challenge by sending the location and a timestamp, the receiver validates the message and compares the timestamp of both messages, if the same timestamp means not malicious attacks. The time synchronized in both sender and receiver, and the response will be sent using infrared rays which make it travel at the speed of light and will be impossible to be altered. The authors suggested using both challenge-response authentication and digital signatures to authenticate the vehicle [16].

- **Timestamp Series**

Timestamp Series technique is used to detect and prevent a Sybil attack in VANETs, with the support of roadside unit (RSU) [5][18]. It is unusual that two vehicles go through various RSUs at the same time with the same timestamp. Accordingly, if vehicle sent a timestamp message that issued by passed RSUs and this message has the same timestamps series with other messages, Sybil attack will be detected. This technique has an issue at road intersections; it may not detect the attack [5][18].

3. Multi-Stage Authentication Algorithm

In this section, we propose a solution to improve the authentication mechanism and keys managements for VANETs, as we mentioned before, using a combination of different techniques will provide a higher security compared to using individual techniques [1]. Therefore, our algorithm is to use more than one stage of cryptography techniques and authenticates the vehicle each time it is switched on. The proposed solution is called "Four Stages Authentication" for the confidential message, while in safety message is called "Three Stages Authentication".

The four cryptography stages in this algorithm are Challenge-Response Authentication, Digital signature, Timestamping, and Encryption. However, in safety messages we do not use the encryption technique since the messages are not confidential, all it matters is if the messages authenticate and deliver fast or not.

3.1 Keys Management

In our solution, we suggest using dynamic key distribution protocol; where for each geographic area there is an RSU Manager manages RSUs in its area, stores all the vehicles keys in its area, and provides the keys to the RSUs when needed.

- **Keys Creation**

The Certificate Authority (CA) will get a request from RSU Manager to create a key to a vehicle whenever the vehicle is switched on in its area, and then the RSU Manager delivers the key to the vehicle through RSU.

- **Keys Revocation**

To revoke a vehicle certificate, the CA will get a request from RSU Manager or legal authority. First the CA checks the lifetime of vehicle certificate, if it is not expired, then the CA will send a message to revoke the vehicle to be stored at the responsible RSU Manager, which will send that message to all RSUs in its area, to deliver it to all the vehicles in their areas. The message will inform the vehicles not to deal with the revoked vehicle and to store the revoked vehicle in Certificate Revocation List (CRL).

When the revoked vehicle goes to another area with new RSU Manager, the new RSU Manager checks the vehicle certificate validity with the old RSU Manager, and then sends the revoked message to all RSUs in its area, to deliver it to all the vehicles in their areas.

- **Keys Distribution**

When the vehicle moves in the same RSU Manager area, the RSU Manager provides the vehicle's key to other vehicles if needed. And when the vehicle goes to another area with new RSU Manager, it will register the vehicle under its authority, after it checks the vehicle certificate validity with the old RSU Manager.

3.2 Authentication Model

In this section, we present the algorithm entities and describe their different properties; the authentication model is shown in *Figure 1*.

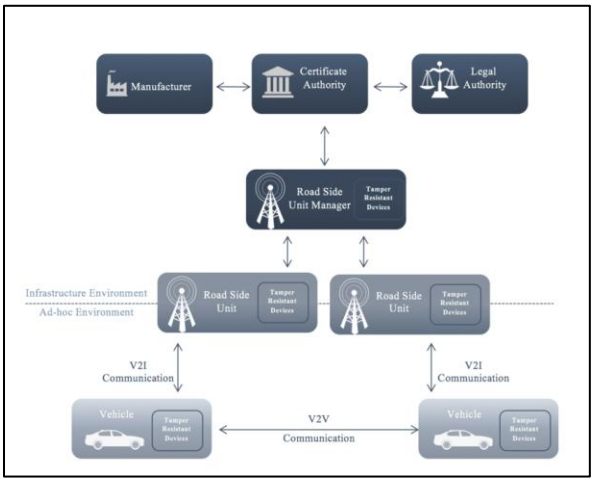

Figure 1: The Authentication Model

Six entities are mentioned and explained below:

- Certificate Authority (CA)
- Legal Authority (LA)
- Tamper Resistant Devices (TRD)
- Road Side Unit (RSU)
- Road Side Unit Manager (RSU Manager)
- Vehicles (V)

- **Certificate Authority (CA)**

The main infrastructure is Certificate Authority, which provides the vehicle with a digital certificate. Initially the vehicle manufacturer provides temporary certificates, then those certificates validated to permanent by government authority CA. In our solution, when the vehicle is switched on, CA provides the vehicle with a digital certificate that consists of a public key, private key, and CA signature. Moreover, when the vehicle is switched off, the vehicle's certificate is revoked and put in Certificate Revocation List (CRL).

CA will provide a public key for all vehicles, whenever the vehicle needs to send an encryption message or to check if the vehicle's certificate is active or revoked. In addition, whatever the receiver detects an attack, the receiver alert CA with the attacker's certificate to revoke it.

Our algorithm improves security and mitigates the problems if the attacker acquired the vehicle's identity. Also, it makes it difficult for the attacker to make brute force attack on the vehicle's certificate. The algorithm could make CRL memory size huge which cause a problem and consume time, but it will not be a concern in our paper.

- **Legal Authority (LA)**

One of the significant infrastructures is Legal Authority, which design regulations that control VANET environment registering the vehicles and handling the malicious attacker legally.

- **Tamper Resistant Devices (TRD)**

For storing sensitive information like the vehicle's private key, we use Tamper Resistant Devices, which will store the secret data, also sign and timestamp the outgoing messages. To provide more security, the TRP has its battery that is recharged using the vehicle's battery, have its synchronized clock and have a set of sensors that prevent an unauthorized entity from tampering with hardware. Unauthorized entity cannot access, erase and modify TRP.

- **Road Side Unit (RSU)**

Road Side Unit in VANETs links the vehicles with CA in term of communication. Also the RSU provides the internet and sends messages such as road condition messages to vehicles nearby. Each RSU has its TRD to store data, sign, encrypt, decrypt, and timestamp messages. Also the sensors in TRD prevent the attacker from tampering with RSU or its operations.

- **Road Side Unit Manager (RSU Manager)**

RSU Managers in VANETs manage all RSUs and vehicles in its geographic area, stores and distribute the vehicles' keys in its area, and provide the vehicle's key to other RSU Managers if needed.

- **Vehicles (V)**

Vehicles in VANETs can be Sender vehicles (SV) and Receiver vehicles (RV). Vehicles can communicate with other vehicles or RSU. Each vehicle has its TRD to store data, sign, encrypt, decrypt, and timestamp messages. Also the sensors in TRD prevent the attacker from tampering with vehicles or its operations.

3.3 Authentication Framework

The authentication framework guides the design of an algorithm to understand its stages and processes, which is shown in *Figure 2*. As it mentioned before, the messages are divided into two types: confidential and safety messages. In confidential messages, we need to provide the confidentiality requirement by encrypting messages applying the public key of the receiver, while in safety messages we do not need that. We have four stages in authenticating confidential messages and three stages in safety messages that are briefly presented below:

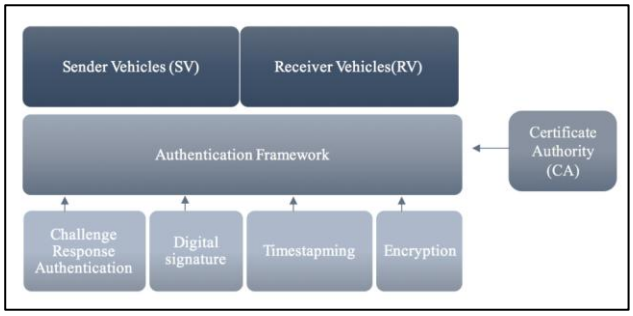

Figure 2: The Authentication Framework

- **First Stage: Challenge-Response Authentication**

The first step of the algorithm starts when the sender wants to send a message to the receiver, the receiver replays with a challenge, to make sure it's not an attacker, the receiver asked the sender for his location and the sender response to the challenge. The receiver checks the validity based on the message round-trip time (RTT), the receiver will accept the communication if the sender in its range.

- **Second Stage: Digital signature**

The second step of the algorithm is signing the message using sender's private key to provide message authentication, message integrity, and message non-repudiation. The vehicle proves that it creates the message and cannot deny that since it uses its private key, and the integrity proves because the digital signature will be different at the receiver side if the message is altered.

- **Third Stage: Timestamping**

Timestamp provides the message integrity, and freshness, which we need if the receiver received the message after the vehicle's certificate is revoked (The vehicle switched off). The receiver will check if the revocation happens after the message timestamped or not, if it happens after the message timestamped, the receiver accepts the message, otherwise he denies it.

- **Fourth Stage: Encryption**

In the algorithm, encrypting the message provides confidentiality, which is needed in confidential messages. The message encrypted using receiver's public key, so unauthorized vehicles cannot access or modify the message. Only the receiver can decrypt the message by applying his private key. This stage is not needed in safety messages because it does not need confidentiality in its messages.
After the fourth stage, the sender sends the timestamped encrypted message and the digital signature to the receiver. The receiver checks the timestamped encrypted message and the digital signature validity. If the message is valid, the receiver will accept it. Otherwise, he denies it.

3.4 Authentication Processes

The authentication process below shows the interactions between vehicles in the sequential order that those interactions occur. *Figure 3, 4, and 5* show the sequence diagrams of two functions of the algorithm: vehicle communication and certification creation and revocation.

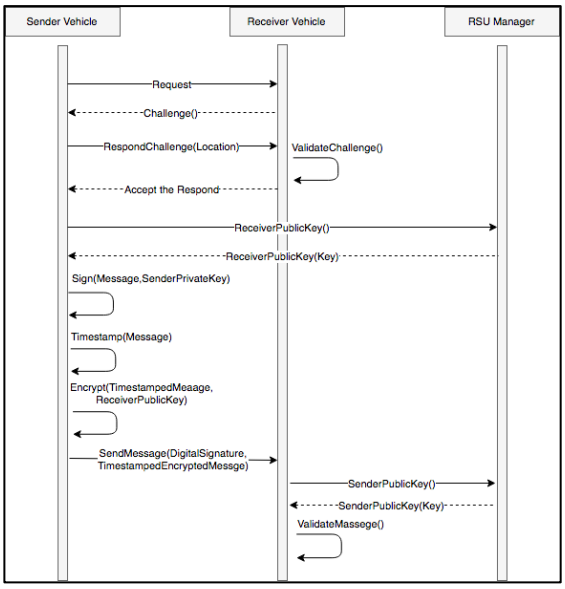

Figure 3: Vehicle Communication Sequence Diagrams (Successful Case)

4. Our Contributions

In the algorithm, our contributions are summarized as follow:

- Certification creation and revocation, which will improve security.
- Putting more than one technique together instead of using one technique provides higher security.
- Develop and implement the challenge-response authentication stage, assuming all other stages are already implemented.

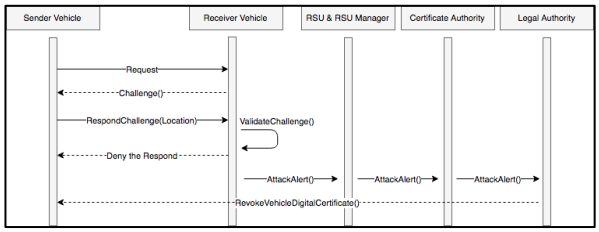

Figure 4: Vehicle Communication Sequence Diagrams (Attack Case)

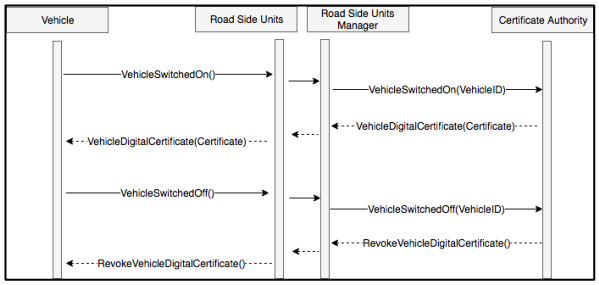

Figure 5: Certification Creation and Revocation Sequence Diagrams

5. Simulation & Performance Analysis

In this section, we implemented challenge-response authentication stage, after assuming all other stages are already implemented. In the implementation, we used OMNET ++ version 5.1 and INET Framework 3.5 in Windows 10. The computer hardware that used in the simulation has an Intel CPU with a speed of 2.7 GHz and 8 GB RAM.
In the simulation, two moving vehicles are wishing to communicate with each other, Vehicles 1 is the sender and Vehicles 2 is the receiver and the communication happen as follows:

- Vehicles 1 starts the communication with Hello message.
- Vehicles 2 responds with a challenge.
- Vehicles 1 responds to the challenge with his location.
- Vehicles 2 accepts or denies the communication based on the round-trip time (RTT), if the RTT in the accepted range which is defined based on the experiment, the message will be accepted, otherwise it will be denied.

The two sections below discuss the simulation parameters that used in the implementation and three different scenarios that considered in our algorithm. The main matrices that used to evaluate the performance of our simulation are delay and accuracy.

5.1 Parameters

Our implementation contains two vehicles that are wishing to communicate with each other using UDP protocol and 802.11p MAC protocol. UDP protocol is more efficient to use in our simulation because it does not consume a lot of time.
Table 1 shows a summary of the simulation parameters. The parameters include vehicles number, transport layer protocol, network layer protocol, vehicles speed limit, vehicles communication range, RTT accepted range and denied range that affects the performance of our algorithm.

Table 1: The Simulation Parameters

Parameters	Value
Number of Vehicles	2
Transport Layer Protocol	UDP protocol
Network Layer Protocol	802.11p MAC protocol
Vehicles Speed Limit	60
Vehicles Communication Range	280m
RTT Accepted Range	0 to 2
RTT Denied Range	3 and higher

5.2 Scenarios

In this section, we present three scenarios: safe, not safe and gray-area communication, which are based on the distance between vehicles 1 and vehicles 2.

- **Safe Communication**

The first scenario used in the simulation has two vehicles with the distance 100m between them, the RTT after the experiment is 1 and the communication is accepted, as shown in *Figure 6*.

- **Not safe Communication**

The second scenario used in the simulation has two vehicles with the distance 541m between them, the RTT after the experiment is 3 and the communication is denied, as shown in *Figure 7*.

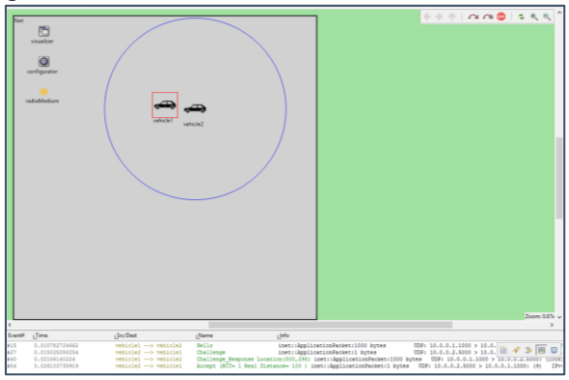

Figure 6: Safe Communication Scenario

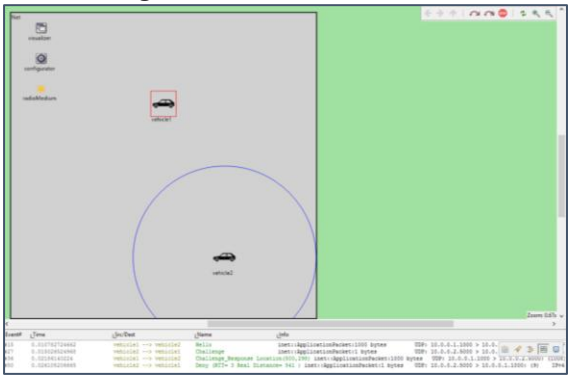

Figure 7: Not safe Communication Scenario

- **Gray-area Communication**

The third scenario used in the simulation has two vehicles with the distance 252m between them, the RTT after the experiment is 3 and the communication is denied, which is not correct since the vehicle 1 is in vehicle 2 range and the distance is less than 280m, as shown in *Figure 8*.

This problem is appearing when the vehicle 1 is in vehicle 2 border range, which we called a gray area; the gray area in our simulation is from 180m to 280m from vehicles 2.

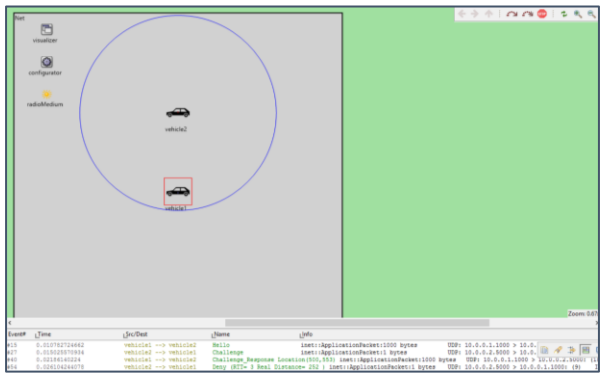

Figure 8: Gray-area Communication Scenario

As a solution, we added a technique called *wait* and *send*, the technique works as follow, when the communication denied the sender could resend the request two times after waiting five seconds. We are waiting five seconds so the vehicles can move and the distance will change accordingly.

After applying *wait* and *send* technique in the third scenario, at the beginning the communication is denied, because the RTT after the experiment is 3. Vehicle 1 starts the communication again after waiting five seconds, the distance becomes 250m between them, the RTT after the experiment is 2 and the communication is accepted, as shown in *Figure 9*.

6. Results &Discussions

In our experiment, the main important matrix to evaluate the performance is the accuracy, which will determine if our algorithm is working correctly or not. Besides, the delay is another important matrix that can affect the VANETs network, in our algorithm the delay will not be an issue since it is a significantly small value and it increases when the distance increases. So, in our experiment we focus on studying and analyzing accuracy matrix.

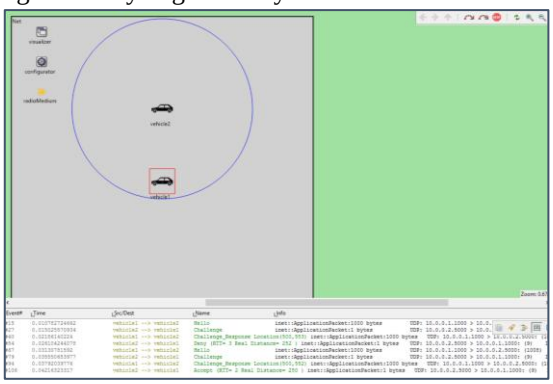

Figure 9: Gray-area Communication Scenario after Wait and Send Technique

Accuracy can affect our algorithm performance, so we experimented 160 times to compare the result and make sure we get the right result. We applied the safe communication

scenario 52 times, not-safe communication 80 times and gray-area communication 28 times. Also, we applied the experiment before and after the *wait* and *sent* technique to compare the result between them.

- **Accuracy, Sensitivity, and Specificity**

In this section, we measure the rating of success by calculating the accuracy, sensitivity, and specificity of our algorithm. Sensitivity or true positive rate (TPR) measures the ratio of the correctly accepted the communication, while specificity or true negative rate (TNR) measures the ratio of the correctly denied the communication. To do that first we need to calculate the true and false positive and the true and false negative, as shown in Table 2.

Table 2: Calculation Outcomes

	Description	**Before *Wait* and *Send* Technique**	**After *Wait* and *Send* Technique**
True Positive (TP)	Correctly accepted the communication	62	75
False Positive (FP)	Incorrectly accepted the communication	0	0
True Negative (TN)	Correctly denied the communication	80	80
False Negative (FN)	Incorrectly denied the communication	18	5

The equations and calculations of sensitivity, specificity, and accuracy before and after the *wait* and *send* technique are:

Before *Wait* and *Send* Technique:

$$\text{Sensitivity} = \Sigma\,TP/\Sigma\,TP + \Sigma\,FN \quad (1)$$
$$= 62 / 62 + 18 = 0.775 \approx 78\%$$

$$\text{Specificity} = \Sigma\,TN//\Sigma\,TN + \Sigma\,FP \quad (2)$$
$$= 80 / 80 + 0 = 1 = 100\%$$

$$\text{Accuracy} = \Sigma\,TP + \Sigma\,TN / \Sigma\,Total \quad (3)$$
$$= 62 + 80 / 160 = 0.8875 \approx 89\%$$

After *Wait* and *Send* Technique:

$$\text{Sensitivity} = \Sigma\,TP/\Sigma\,TP + \Sigma\,FN \quad (4)$$
$$= 75 / 75 + 5 = 0.9375 \approx 94\%$$

$$\text{Specificity} = \Sigma\,TN//\Sigma\,TN + \Sigma\,FP \quad (5)$$
$$= 80 / 80 + 0 = 1 = 100\%$$

$$\text{Accuracy} = \Sigma\,TP + \Sigma\,TN / \Sigma\,Total \quad (6)$$
$$= 75 + 80 / 160 = 0.96875 \approx 97\%$$

From the calculation above, at the beginning as shown in Figure 10 and calculated from Equation (3), the accuracy was 89% and the errors in the experiment were 11%, which is high, these errors were in the gray area where the vehicle is in border range of the other vehicle. While the sensitivity calculated from Equation (1) was 78% meaning that we correctly accepted 78% of the communication. So, as a solution to enhance our algorithm, we applied *wait* and *send* technique.

After applying *wait* and *send* technique as shown in *Figure 11*, and calculated in Equation (6), the accuracy became 97% and the errors in the experiment became 3%, the reason why the errors decreased is that when the vehicles wait for five seconds and then send, it moves and the distance and the RTT change based on vehicles directions.

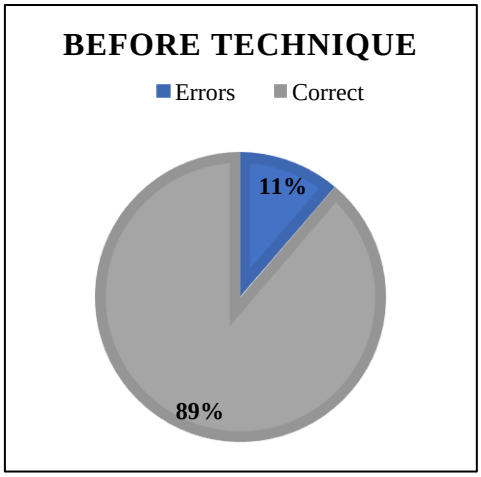

Figure 10: Accuracy without Wait and Send Technique

The sensitivity calculated from Equation (4) was 94% meaning that we correctly accepted 94% of the communication.

The specificity of our algorithm calculated in Equation (2) and (5) were 100%, which means we have denied all unsafe communications correctly, thus provides more security.

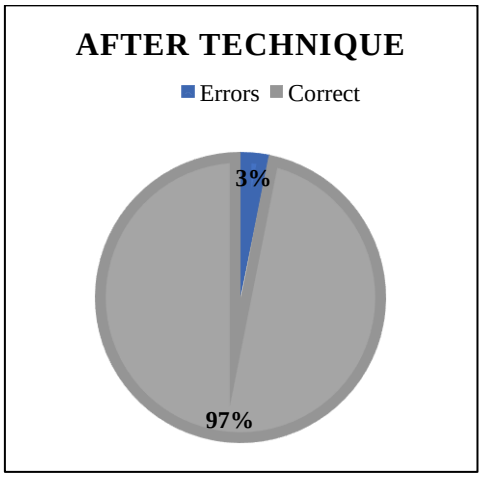

Figure 11: Accuracy with Wait and Send Technique

7. Conclusion

Vehicular Ad-hoc Networks (VANETs) are developed to enhance the safety of roads and vehicles services. Given their significance relevance to the drivers' lives, it attracts many adversaries to attacks the network, which cause huge consequences to vehicles. Therefore, VANET security causes a great challenge, especially authentication since it is the first step of communication.

In this paper, we apply cryptography in authentication to improve security. The proposed authentication algorithm provides more security since it is used more than one stage of cryptography techniques and the certification creation and

revocation each time when vehicle switched on and off. The stages are a challenge-response authentication, digital signature, time-stamping, and encryption. Our algorithm uses the following techniques: challenge-response to provide authentication, digital signature to provide authentication, message integrity, and message non-repudiation, timestamping to provide integrity and freshness, and finally encryption to provide confidentiality.

Our algorithm at the beginning provides 89% accuracy, which we enhanced by adding *wait* and *send* technique that allows the vehicle to wait for five seconds and then resend again, the accuracy became 97%. The delay will not cause a problem because it is significantly a small value. Therefore, our algorithm will provide security, integrity, message non-repudiation, freshness, confidentiality, and authentication.

There are some limitations faced us in this paper, listed as follows:

- Since the certification revocation happens whenever the vehicle switched off, CRL memory size will be huge, which may cause a problem and consume time.
- The proposed four stages authentication will consume a huge memory size and power.

As a future work, we will try to improve the accuracy of the algorithm to 100%. We will implement the other three stages then measure and evaluate the result from the implementation. In addition, we will use more than two vehicles in the simulation.

References

[1] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions", Vehicular Communications, vol. 1, pp. 53-66, 2014.

[2] M. N. Rajkumar, M. Nithya, and P. HemaLatha, "Overview of Vanet with Its Features and Security Attacks", International Research Journal of Engineering and Technology (IRJET), vol. 03, no. 1, pp. 137-142, 2016.

[3] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", Telecommunication Systems, vol. 50, pp. 217-241, 2012.

[4] T. Sukuvaara and C. Pomalaza-Ráez, "Vehicular Networking Pilot System for Vehicle-to-Infrastructure and Vehicle-to-Vehicle Communications", International Journal of Communication Networks and Information Security (IJCNIS), vol. 1, no. 3, pp. 1-11, 2009.

[5] M. Rahbari and M. A. J. Jamali, "Efficient detection of sybil attack based on cryptography in VANET," International Journal of Network Security & Its Applications (IJNSA), vol. 3, pp. 185-195, 2011.

[6] Arabiya. "المرور حوادث في عالمياً الأولى السعودية". Available: https://www.alarabiya.net/ar/saudi-today/2013/03/13/السعودية-المرورية-الحوادث-في-عالمياً-الأولى.html, Mar. 13, 2013 [Accessed on Oct. 4, 2016].

[7] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET", International Journal of Network Security & Its Applications, vol. 5, p. 95-105, 2013.

[8] Y. Toor, P. Muhlethaler, A. Laouiti, and A. De La Fortelle, "Vehicle ad hoc networks: applications and related technical issues", IEEE communications surveys & tutorials, vol. 10, pp. 74-88, 2008.

[9] A. Sari, O. Onursal, and M. Akkaya, "Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)", International Journal of Communications, Network and System Sciences, vol. 8, p. 552-566, 2015.

[10] S. S. Kumar, "Vehicular Ad Hoc Network", International Journal of Computer, Information, Systems and Control Engineering, vol. 8, no. 4, pp. 627-630, 2014.

[11] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys", Computer Communications, vol. 44, pp. 1-13, 2014.

[12] X. Lin, R. Lu, C. Zhang, H. Zhu, P.H. Ho, and X. Shen, "Security in vehicular ad hoc networks", IEEE communications magazine, vol. 46, pp. 88-95, 2008.

[13] H. Hartenstein and L. Laberteaux, "A tutorial survey on vehicular ad hoc networks", IEEE Communications magazine, vol. 46, pp. 164-171, 2008.

[14] I. A. Sumra, I. Ahmad, and H. Hasbullah, "Classes of attacks in VANET", Proceeding of Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, pp. 1-5, 2011.

[15] T. Sukuvaara, K. Mäenpää, R. Ylitalo, H. Konttaniemi, J. Petäjäjärvi, J. Veskoniemi, and M. Autioniemi, "Vehicular Networking Road Weather Information System Tailored for Arctic Winter Conditions", International Journal of Communication Networks and Information Security (IJCNIS), vol. 7, no. 1, pp. 60-68, 2015.

[16] A. Dahiya and V. Sharma, "A survey on securing user authentication in vehicular ad hoc networks", International Journal of Information Security, vol. 1, pp. 1-9, 2001.

[17] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications," IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, vol. 13, pp. 8-15, 2006.

[18] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, vol. 15, pp. 39-68, 2007.