Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 198 (2022) 276–281

Procedia Computer Science

www.elsevier.com/locate/procedia

International Workshop on Computational Intelligence and Cybersecurity in Emergent Networks
(CICEN 2021)
November 1-4, 2021, Leuven, Belgium

Secure Authentication Scheme for 5G-based V2X Communications

Meriem Houmer*, Mariyam Ouaissa, Mariya Ouaissa

Moulay Ismail University, Marjane 2, BP: 298, Meknes 50050, Morocco

Abstract

Information and communication technologies applied to means of transport allow the design and development of new applications and bring new solutions for the mobility of people. All these applications are grouped within the field of Intelligent Transport Systems (ITS) and improve user mobility in terms of safety, reliability, capacity, and quality. Vehicle to Everything is a novel technology of ITS which aims to enhance the security and efficiency of road traffic by using wireless communications. Cellular communications networks such as LTE-V2X and 5G NR, integrated into the Vehicle to Everything (V2X) architecture designed to support vehicular communications and deployed on a large scale, appear in particular to be a relevant solution. They could indeed guarantee reliable geographic distribution and acceptable performance (latency, bandwidth, packet loss). In this context, we propose a secure authentication scheme for 5G-based V2X communication. Our solution aims to guarantee a high level of security in different types of vehicular communication (V2V, V2I, V2N) to achieve the security requirements using lightweight cryptographic methods and to support vehicles to receive securely all keys and messages from RSU, other vehicles, or network. To validate our proposal, we utilize the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool to achieve the security goals, also we evaluate the performance according to the operational cost which demonstrates that our model has a less computational cost.

Keywords: Type your keywords here, separated by semicolons ;

* Corresponding author.
E-mail address: houmer.m@gmail.com

10.1016/j.procs.2021.12.240

1. Introduction

In recent years, the automotive world has increasingly relied on wireless communications systems in order to me
In recent years, the automotive world has increasingly relied on wireless communications systems in order to meet safety requirements. A new concept dedicated to the development of transport systems has emerged: Intelligent Transport Systems (ITS). ITS consist of exploiting the various technologies (electronics, telecommunications, information processing, and control) which will revolutionize the interfaces between the vehicle, the driver, and the road. ITS covers many facets where wireless communications play a role of paramount importance. As a result, car manufacturers are increasingly committed to making their vehicles capable of communicating over wireless links. As human lives are at the forefront of all stakeholders, road safety applications have two major requirements - speed and reliability which must be met by the underlying communication network [1].

Over the past decade, the connected vehicle paradigm has aroused great interest from academia, governments, industry, and standards organizations. The interaction between the vehicle and the road environment is at the heart of many ITS applications; this requires the development of efficient Vehicle to Everything (V2X) communication systems and higher precision positioning systems. V2X encompasses Vehicles to Infrastructure (V2I) communication, Vehicle to Vehicle (V2V) communication, and Vehicles to Network (V2N) communication [2].

Cellular networks are the other approach considered for the deployment of vehicular communication networks. These cellular networks have an important advantage over ITS-G5 networks: an existing large-scale deployment guaranteeing good coverage. They are also able to provide decent data throughput and latency. Two generations of cellular communications networks could allow the deployment of high-performance vehicular communications: 4G networks (LTE-V2X) and 5G networks [3].

It is crucial that the information exchanged between the various actors of the V2X system is reliable and exact in order to guarantee a certain number of objectives such as authentication, integrity, confidentiality, and privacy. In this context, we propose a secure and lightweight scheme for 5G-based V2X communication in different types of vehicular communication namely V2V, V2I, and V2N. In our solution, we use Elliptic-Curve Cryptography (ECC) and Attribute-based Signature (ABS) to ensure the security of keys and messages exchanged between vehicles or vehicles and RSU, in the other side we consider an improved version of authentication and key agreement protocol based on Elliptic Curve Diffie Hellman (ECDH) for 5G system to surmount standard authentication protocol 5G-AKA limitation.

The rest of this paper will be presented as follows: the next section describes the system model. Section 3 presents the different steps of our scheme. We analyze the security and performance evaluation in terms of the operational cost of our proposed in Section 4. Finally, we draw our conclusions.

2. System Model

V2X communication encompasses the exchange of data between vehicles but also with infrastructure. This is for the purpose of improving road safety and increasing traffic efficiency, as depicted in Fig. 1 that presented the system model combining two networks; vehicular communication and 5G cellular system. The purpose of this communication is to reduce environmental impacts and provide additional services and information to travelers.

To allow communications to be established between the various components integrated into vehicle networks, the standardization of many types of communication is necessary [4]:

- Vehicle-to-Vehicle (V2V): these are a direct wireless communication between On-Board Units (OBUs).
- Vehicle-to-Infrastructure (V2I): these are communications between a vehicle and equipment belonging to the roadside infrastructure: RSU, road lighting, traffic sign, radar, stop bus, etc.
- Vehicle-to-Network (V2N): these are communications between a vehicle and equipment belonging to the cellular communication network, particularly Base Station (BS).
- Vehicle-to-Person (V2P): these are communications between a vehicle and a non-motorized road user: pedestrian, cyclist, etc.

The 5G architecture contains two major parts: New Generation Radio Access Network (NG-RAN) and a 5G Core (5GC) network. The first one includes the new Generation Node Base (gNB) station that connect devices vehicles with the core network. For the 5G network core is based on the breakdown of the control plane and the user plane, it consists of different entities that ensure authentication, mobility and signalization [5].

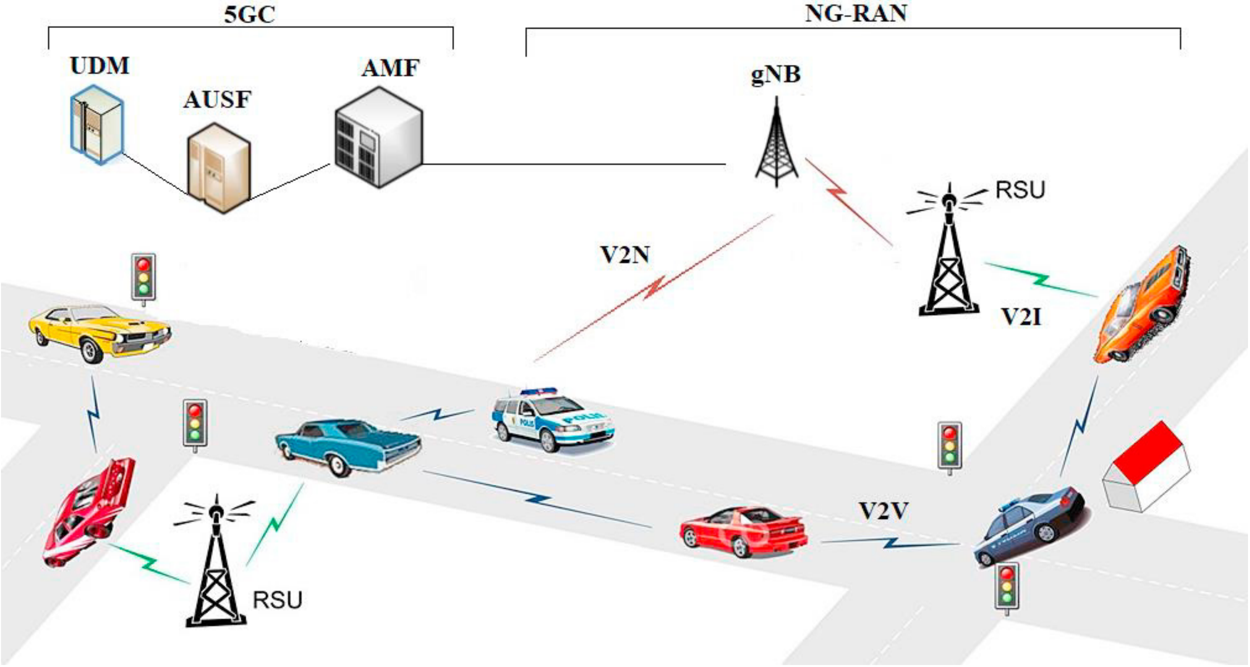


Fig. 1. System Model.

3. Proposed Scheme

In this paper, we propose a 5G based V2X communication security model, which consists to ensure reliable and secure authentication between vehicles, Infrastructure and 5G network.

3.1. Vehicle to Infrastructure

In this case, each vehicle is authenticated with RSU without a trusted third party authority. We consider an ECDH algorithm to ensure vehicle authentication via RSU and the digital signature algorithm based on attributes to sign the messages by vehicles. The aim to use elliptic curves and attributes algorithms is their faster processing compared to others cryptographic methods.

The Fig. 2 illustrates the procedure of authentication and communication between vehicle and RSU. Still, The description in detail of all steps is as follows:

- The vehicle Vi and RSU choose together an elliptical curve E (a, b, K) and a point P on the curve
- Vi secretly chooses k_{Vi} and calculates $k_{Vi}.P$
- RSU secretly chooses k_{RSU} and calculates $k_{RSU}.P$
- Vi and RSU calculate the shared secret $Ss=k_{Vi}.k_{RSU}.P$
- The authentication of the vehicle by the RSU is ensured by the ABS signature process using the private key KPR and the ABS verification using the public key KPUB.

With KPR_{Vi} is k_{Vi} $KPUB_{Vi}$ is E (a, b, K), P and k_{Vi}
KPR_{RSU} is k_{RSU} $KPUB_{RSU}$ is E (a, b, K), P and k_{RSU}

For data transmission between vehicles, we use elliptical curve encryption algorithm to guarantee that the message authentication is establish with success as shown in Fig. 3.

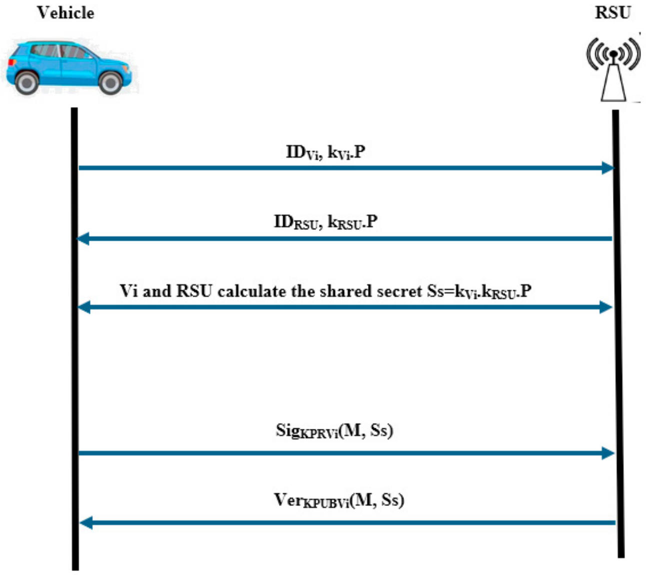


Fig. 2. Authentication and Communication between Vehicle and RSU

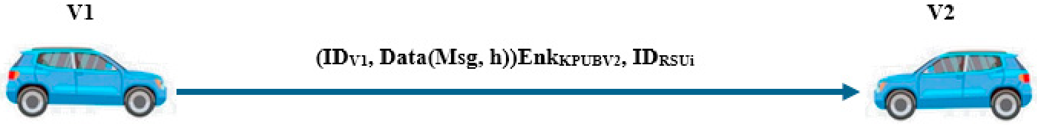


Fig. 3. Communication between Vehicles

3.2. Vehicle to Network

In vehicle to network communication, we suggest to improve an authentication and key agreements protocol for 5G network to overcome standard authentication protocol 5G-AKA limitation [6]. Our proposed protocol pursues 5G cellular network architecture and resists many threats including replay attack, redirection attack, man in the middle attack and DoS attack (Fig. 4).

Actually, in our proposal, the authentication process and key agreements are established between vehicles, AMF/SEAF, AUSF, and UDM/ARPF. Each vehicle has a permanent identity called SUPI that the provider has to install which permits the user to register in the 3GPP core network. We regard the Elliptical Curve Diffie Hellman Key Agreement protocol, which provides for the establishment of a shared secret key via an unsecured channel, and utilize symmetric encryption in order to encrypt the identity, for the purpose of obtaining a Subscription Concealed Identifier (SUCI) that hidden the SUPI calculated by the UE.

In addition, we assume that communication between core network entities and security functions (AMF/AUSF/ARPF) is secure, and long-term IPSec, (D)TLS, or DIAMETER sessions are maintained across established channels between identified entities.

4. Validation and Evaluation

In this section, we analyze the formal verification of our model and we evaluate the performance in terms of operational cost.

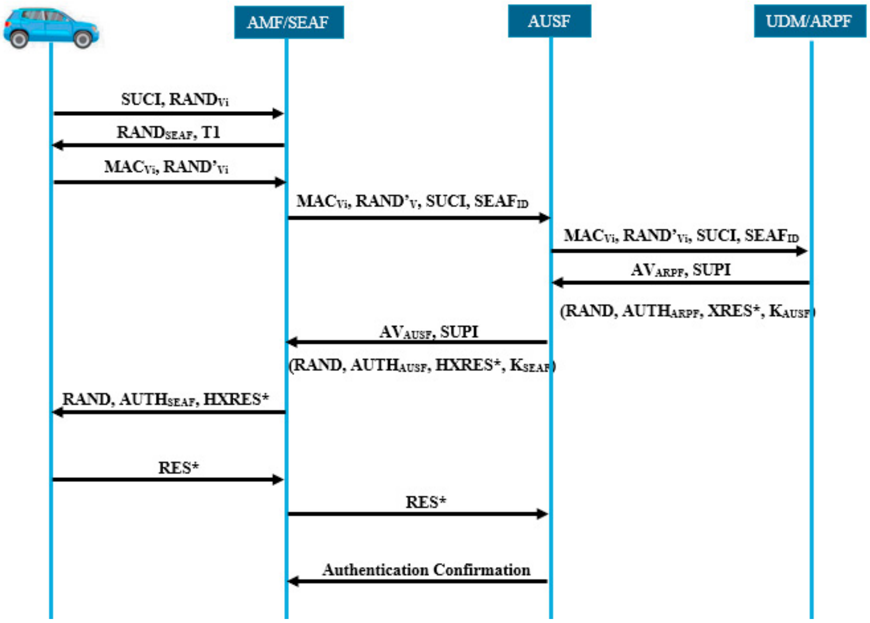
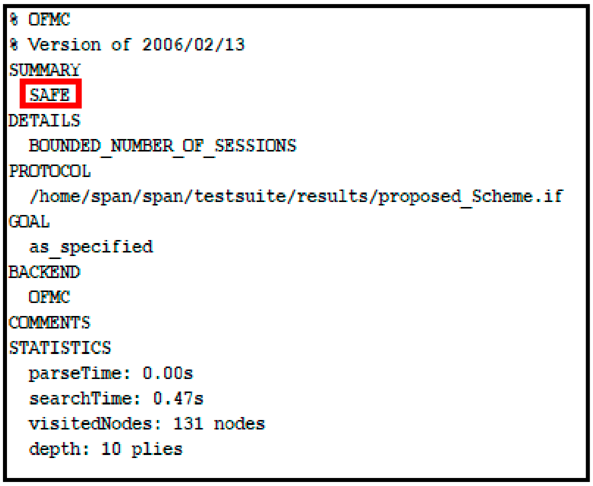

AMF/SEAF
AUSF
UDM/ARPF
SUCI, RAND$_{Vi}$
RAND$_{SEAF}$, T1
MAC$_{Vi}$, RAND'$_{Vi}$
MAC$_{Vi}$, RAND'$_{V}$, SUCI, SEAF$_{ID}$
MAC$_{Vi}$, RAND'$_{Vi}$, SUCI, SEAF$_{ID}$
AV$_{ARPF}$, SUPI
(RAND, AUTH$_{ARPF}$, XRES*, K$_{AUSF}$)
AV$_{AUSF}$, SUPI
(RAND, AUTH$_{AUSF}$, HXRES*, K$_{SEAF}$)
RAND, AUTH$_{SEAF}$, HXRES*
RES*
RES*
Authentication Confirmation

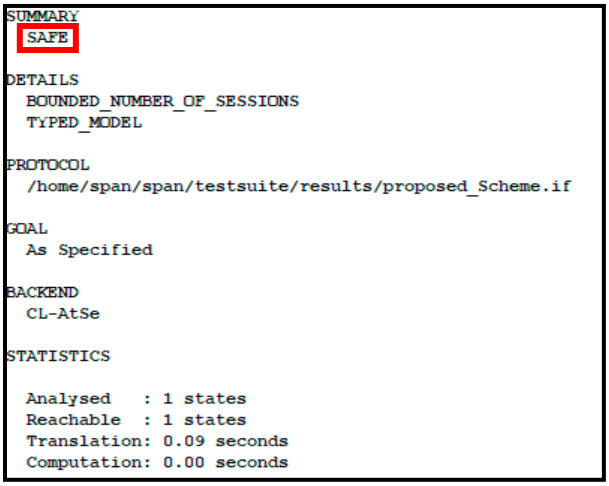
Fig. 4. Improved 5G-AKA for V2N Communication

4.1. Security Analysis

Our scheme was verified by a tool of security verification, Automated Validation of Internet Security Protocols and Applications (AVISPA) [7] which supports automatic and rigorous validation of internet security protocols. The main principle of our model is to assure security requirements such as mutual authentication, integrity, confidentiality between the vehicles, RSU and the equipment of 5GC network (SEAF, AUSF and ARPF). In fact, Figs. 5 and 6 present the specification of our model using two backends OFMC and CLAtSe respectively, according to these figures we can conclude that our solution achieves the goal of security and can overcome many malicious attacks.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/proposed_Scheme.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.47s
  visitedNodes: 131 nodes
  depth: 10 plies
```



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/proposed_Scheme.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 1 states
  Reachable  : 1 states
  Translation: 0.09 seconds
  Computation: 0.00 seconds
```

Fig. 5. OFMC Back-End results report

Fig. 6. CL-AtSe Back-End results report

4.2. Operational Cost

To evaluate the performance of our system in terms of operational cost, we choose to implement the execution time values of all cryptographic algorithms and operations considering our solution and other existing ones using Crypto++ Library [8] running on a test platform with 2.1 GHz processor using Ubuntu. Table 1 shows that our used operations are faster and more efficient.

Table 1. Execution Time of Algorithms/Protocols.

Operations	Algorithms/Protocols	Execution Time (μs)
Key Exchange	DH	2
	ECDH	1.29
	DSA	2.47
Digital Signature	ECDSA	5.38
	ABS	1.2
	RSA	6.28
Asymmetric Encryption	El-Gamal	5.97
	ECC	4.33

5. Conclusion

The deployment of vehicular communication networks today appears to be a relevant solution to ensure the safety of road users and make road traffic more fluid. In an effort to improve road safety, vehicles are becoming increasingly intelligent and able to detect potentially dangerous obstacles. It is therefore necessary to share information between vehicles (V2V) on the one hand and between vehicles and infrastructure (V2I) and (V2N) on the other hand. Among the problems that have arisen in these networks is the problem of authentication and confidentiality of data transmitted between entities. Our scheme allows vehicles to establish secret key and authenticate in RSU in a reliable way using digital signature by ABS algorithm and also secure the communication between vehicles using the cryptographic keys obtained in the phase of key exchange by ECDH. In addition, our proposed consist to improve an authentication and key agreement protocol for 5G network to ensure security and overcome the limitations of existing 5G-AKA in V2N communication.

References

[1] Dimitrakopoulos George, and Demestichas Panagiotis. (2010) “Intelligent transportation systems.” *IEEE Vehicular Technology Magazine* **5(1)**: 77-84.

[2] Jgian Wang, Yameng Shao, Yuming Ge, and Rundong Yu. (2019) “A survey of vehicle to everything (V2X) testing.” *Sensors* **19(2)**: 334.

[3] El Faouzi Nour-Eddin, Leung Henry, and Kurian Ajeesh. (2011) “Data fusion in intelligent transportation systems: Progress and challenges–A survey.” *Information Fusion* **12(1)**: 4-10.

[4] Hakeem Shimaa A. Abdel, Hady Anar A., and Kim HyungWon. (2020). “Current and future developments to improve 5G-NewRadio performance in vehicle-to-everything communications.” *Telecommunication Systems 75***(3)**: 331-353.

[5] Ouaissa Mariya, Houmer Meriem, Ouaissa Mariyam. (2020) “An Enhanced Authentication Protocol based Group for Vehicular Communications over 5G Networks.” In *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*. pp. 1-8. IEEE.

[6] Ouaissa Mariya and Ouaissa Mariyam. (2020) “An Improved Privacy Authentication Protocol for 5G Mobile Networks.” In *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)*. pp. 136-143. IEEE

[7] AVISPA Project: http://www.avispa-project.org/

[8] Crypto++ Library: http://www.cryptopp.com/