Indonesian Journal of Electrical Engineering and Computer Science
Vol. 34, No. 1, April 2024, pp. 396∼406
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v34.i1.pp396-406

Formal validation of authentication scheme in 5G-enabled vehicular networks using AVISPA

Mays A. Hamdan, Amel Meddeb Maklouf, Hassene Mnif
École Nationale d'Electronique et des Télécommunications (ENET'com) Sfax, University of Sfax, Sfax, Tunisia

Article Info

Article history:

Received Nov 18, 2023
Revised Dec 26, 2023
Accepted Jan 14, 2024

Keywords:

5G-assisted vehicular network
Authentication
AVISPA
Elliptic curve cryptography
Formal validation

ABSTRACT

Smart transportation may come from 5G-enabled cars. Traffic reports include congestion, roads, and driving. Urbanisation and population growth increase traffic accidents and travel time. Traffic accidents kill and injure most people worldwide. Intelligent transportation systems (ITS) improves driver and pedestrian safety. This study connects the VANET to 5G to create a 5G-enabled vehicle network because the road-side unit (RSU) is expensive and unsecure. This study connects numerous automobiles to TA for 5G-BS D2D communication. Data transmissions between autos are risky. Several scholars suggest authentication techniques for safe vehicle-to-vehicle communications. Overhead may enable side-channel attacks with these tactics. A secure and effective efficient and secure authentication-privacy-preserving (ES-APP) system connected TA, 5G-BS, and on-border unit (OBU) was presented. Initialization, vehicle registration, parameter renewal, message signing, single and batch verification are ES-APP steps. The formal evaluation automated verification of internet security protocols and applications (AVISPA) tool with on-the-fly model-checker (OFMC) and attack searcher (ATSE) back-ends secures the suggested ES-APP technique. ES-APP appears impervious to active and passive AVISPA assaults.

Corresponding Author:

Amel Meddeb Maklouf
École Nationale d'Electronique et des Télécommunications (ENET'com) Sfax, University of Sfax
Sfax, Tunisia
Email: amel.makhlouf@enetcom.usf.tn

1. INTRODUCTION

The vehicular ad-hoc network (VANET) is a wireless communication system network that operates autonomously and independently of infrastructure, and is often thought of as a sibling of the mobile ad-hoc network (MANET) [1]–[4]. Because it involves the interconnection of several autonomous car sensors and other types of heterogeneous components, it can be classified as an internet of things (IoT) application. The idea that vehicles can band together in ad-hoc networks to better share information about hazards and make daily commutes easier was first proposed in 2001. Since the early 2000 s, researchers have been hard at work developing VANET into a more practical and user-friendly network design [5]–[8]. The system is mobile because it relies on moving vehicles, each of which acts as a relay station or information hub, and it can be built on top of any wireless networking technology (typically short range radio technologies like wireless local area network (WLAN)) and can also use visible light communication to link its various nodes and enable constant data relay and exchange of traffic details. It can be of great use in warning people about the weather, avoiding traffic bottlenecks, and even avoiding accidents [9]. According to the numbers, the peak data transmission rate over 5G wireless networks can exceed 20 Gb/s while the average rate is well above 100 Mb/s. The supported network is capable of offering a more stable connection and has a capacity one thousand times that of existing networks [10]–[12]. Because VANET is a wireless network, it is more susceptible to a variety of assaults, including impersonation attacks, message intercept attacks, modification attacks, and more. Attacks like these might cause authorities or drivers to make poor choices, and they can also be used inappropriately [13], [14]. An attacker could, for instance, pry into a victim's private life by intercepting and reading a communication, or cause traffic lights to change to green without actually causing an emergency by altering a message to indicate such [4], [13], [15]. For this reason, the study proposes an authentication mechanism for 5G-enabled vehicle networks to combat these problems. Initialization, vehicle registration, parameter renewal, message signing, single verification, and batch verification are the six processes that make up the proposed efficient and secure authentication-privacy-preserving (ES-APP) approach. We use automated verification of internet security protocols and applications (AVISPA) to show that our security model is secure once it has been formally validated. The following is the paper's most significant original contribution: (i) for 5G-enabled vehicle networks, we propose an authentication scheme with the following steps: initialization; vehicle registration; parameter renewal; message signing; single verification; batch verification; and (ii) we provide formal validation of the proposed scheme by using AVISPA.

The remainder of this paper is organized as follows. In section 2, this paper review the literature review studies for the vehicular system. In section 3, we provide the description of the system model and security attacks model of this paper. In section 4, we propose the authentication scheme. In section 5, we analysis formal validation of the suggested solution utilising AVISPA. Lastly, this work is concluded in section 6.

2. LITERATURE REVIEW

In 5G-enabled vehicle networks, Al-Mekhlafi *et al.* [16] provided a lightweight quantum-resistant approach based on the lattice method to cope with these problems. In place of operations-based elliptic curve encryption or bilinear pair cryptography, their solution utilises matrix multiplication to create and validate signatures for messages that are shared between drivers. Chen *et al.* [17] addressed the need for anonymous authentication by recreating a short group signature technique that is both secure and effective for establishing a trail of origin within a given domain. They then proposed BCGS, an integrated blockchain and group signature system, as a secure, privacy-preserving, cross-domain authentication protocol for VANETs. For BCGS,cross-domain vehicle authentication is made possible through the use of blockchain technology, and conditional privacy is ensured through the use of a group signature system. Al-Mekhlafi *et al.* [18] suggests an authentication approach using fog computing as a means to address these concerns in 5G-assisted vehicle systems. To implement this approach, they proposed using a fog server to generate public anonymity identities and signature keys, which are then preloaded into each verified vehicle. Using homomorphic encryption, automobiles in this approach broadcast their encrypted driving paths to a fog node via Zhang *et al.* [19]. In order to manage traffic without having access to each vehicle's specific route information, the traffic management centre (TMC) decrypts the accumulated ciphertexts sent from the fog node. Additionally, public key management for automobiles is handled by blockchain in this approach. Their thorough research and security verification suggest that their solution can accomplish the security goals of VANETs [20].

For mobile fog computing over 5G systems, Mohammed *et al.* [21] proposed a new anonymous authentication technique we call ANAA-fog. In order to verify digital signatures in the proposed ANAA-fog method, a fog server generates a temporary secret key for each participating vehicle. ProfVerif was used to test the security of the ANAA-fog scheme's signing method. This research fulfilled many needs for confidentiality and safety. Among these include the ability to withstand tampering, forgery, replay, and man-in-the-middle attacks, as well as the ability to maintain privacy under certain conditions. To address these concerns, Alazzawi *et al.* [22] proposed an identity-based privacy-preserving authentication technique (ID-PPA) for use in VANETs. ID-based security techniques for VANETs have seen widespread use as of late. There could be many issues with these plans, though. ID-PPA method does, in fact, solve these issues that are typical of ID-based schemes. However, unlike previous ID-based methods, the ID-PPA scheme does not suffer from the key escrow issues and impersonation assaults. Further, it offers a practical method for tracking down and removing any harmful vehicle from the network. Al-Mekhlafi *et al.* [23] proposed a fog computing technique enabled on the polynomial of Chebyshev that enables the removal of anonymous in 5G-assisted vehicle systems. Using fog computing, we've developed a system that makes insider attacks impossible. Specifically, the fog server does not renew the signature key once a pseudonym ID's validity term is set to expire. Bayat *et al.* [24] proposes a novel authentication method that is both efficient and novel for use in VANETs. The proposed solution lets vehicles authenticate each other without a group of signers, an active road side unit (RSU) network, a secret key, or other protections. For 5G-assisted vehicular fog computing, Al-Shareeda and Manickam [25] offered a COVID-19 vehicle built on an efficient mutual authentication system. The suggested system employs two different values for the special flag: SF=0 for typical vehicles and SF=1 for COVID-19 vehicles. The proposed strategy achieves the aims of COVID-19 and medicine without compromising the confidentiality of individual patients. For vehicle-to-vehicle (V2V) communications on VANETs, Bansal *et al.* [26] presented an identity-based computationally efficient privacy-preserving authentication (ID-CEPPA) method based on identity-based cryptography (IDC) and elliptic curve cryptography (ECC). The method ensures source authentication, message integrity, non-repudiation, and anonymity of vehicles for secure and reliable V2V interactions. In addition, their method supports batch-signatures verification, which enables the authentication of several messages all at once. In this research, Al-Shareeda *et al.* [27] offered a secure and efficient conditional privacy-preserving authentication (SE-CPPA) technique for protecting against impersonation attacks and improving performance. The proposed SE-CPPA system employs bilinear pair cryptography for message signing and verification.

Through security analysis and comparison, the suggested SE-CPPA approach can accomplish security goals in terms of formal and informal analysis. In order to prevent impersonation attempts, the tamper-proof device (TPD) contains only the most recent, verified, and legitimate information on the vehicle. Since the proposed SE-CPPA approach does not rely on the MapToPoint hash function or a large number of cryptographic operations, it offers significant savings over previous schemes in terms of processing and transmission costs. To ensure confidential transmissions on VANET, Alshudukhi *et al.* [28] suggested a scheme that combines a minimal authentication protocol with conditional privacy protection. The proposed method is highly suited for dealing with security and privacy issues because it combines the TPD based schemes with the roadside unit (RSU) based schemes. The suggested method involves initial public parameters and keys of the system being preloaded onto each TPD of the RSU as opposed to the TPD of the on-border unit (OBU). For 5G-enabled vehicle networks, Al-Shareeda *et al.* [29] presented a safe and efficient data-sharing mechanism that does not require RSU. Their process consisted of six steps: initialising the TA (TASetup), generating a pseudonym identification (PIDGen), creating a key (KeyGen), signing a message (MsgSign), verifying a single signature (SigVerify), and verifying a batch of signatures (BSigVerify). They presented a vehicle that can validate several signatures at once. Their solution not only meets privacy and security goals, but it is also resilient against common vehicle-network security threats.

3. BACKGROUND

3.1. System model

The system model of this paper is proposed, as shown in Figure 1. There are three main components in the system. These components are trusted authority (TA), 5G-base station (5G-BS), and OBU. The description of these components is as follows. (i) TA: a neutral third party, it is the sole organisation with access to decrypted OBU identities. The system's parameters are generated by this component, which has extensive computing and storage capabilities [8]. (ii) 5G-BS: are wireless devices that are mounted on roadside infrastructure such as traffic lights; they connect with passing vehicles through the 5G standard, relay those transmissions to the TA for verification and processing, and cannot also do some of those tasks locally as our assumption; (iii) OBUs: are installed in all vehicles; they are hidden and cannot be interfered with. The DRSC protocol and 5G standard allow OBUs, which are wireless logical units, to communicate with one another and with TA.

3.2. Security model

The security model of the proposed scheme is provided. These models as forgery, replay, modify, and man-in-the-middle attacks. The description of these attacks is as follows; (i) forgery: the attacker launch forgery attacks to impersonate authentic identify of enrolled vehicles in order to disturb the system, (ii) replay: the attacker launch replay attacks to replay the message sent from authentic vehicles in different times for disturbing the system, (iii) modify: the attacker launch modify attacks to modify the message sent via authentic vehicles in order to disturb the system, and (iv) man-in-the-middle (MITM): the attacker launch MITM attacks to capture the message sent via both authentic vehicles in order to disturb the system.

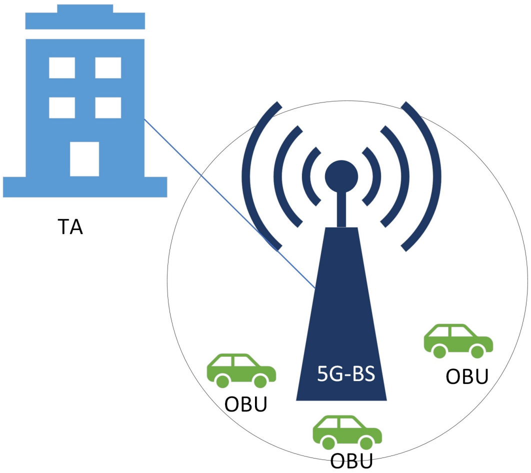


Figure 1. System model of proposal ES-APP scheme

4. PROPOSED METHOD

In this paper, we detail the ES-APP method, a proposed approach to lowering the system's overhead while maintaining security and privacy. The six steps that make up the proposed ES-APP approach are initialization, vehicle registration, parameter renewal, message signing, single verification, and batch verification. The subsequent sections go into detail regarding these phases.

4.1. Initialization

During this stage, TA is in charge of generating the following security parameters: elliptic curve, encryption/decryption, and hash functions. The TA selects two extremely large prime numbers, p and q, as well as an additive group G of rank q and generator P. All points on the elliptic curve E defined by the formula $y2 = x3 + axe + b$ mod p, with a and b satisfying the condition F_p are members of the additive group G. The TA generates a random number, $sinZ_q$, to use as the private key, and uses $Pub = s.P$ to determine the public key. The symmetric encryption and decryption $ENC(.)/DEC(.)$ function, as well as the cryptographic hash function h_1, are both selected by the TA. By default, TA makes the values for $Pub, h_1, p, q, G, ENC(.), DEC(.), a, b$ available to the public.

4.2. Vehicle registration

Now is the time to register your vehicle with TA before it rolls off the assembly line. TA computes a list of pseudonym-IDs and necessary signature keys according to a short valid duration before preloading the public parameters. The OBU car will already be equipped with these settings. First, the user establishes trust between themselves and the TA by providing credentials (such as their RID_v and password PW) through an encrypted connection. Personal information is recorded in the TA database with car registrations. Using the formula $ps = h_1(RID_v||s||d)$, where d is a random number, the TA generates a pseudonym to safeguard and renew RID_v. The TA will save d and RID_v in the vehicle registration list for the renew parameters phase. The TA generates a set of pseudonym-IDs and related signature keys and preloads them into the OBU. Pseudonym-IDs are listed as follows: $LPIDv = "LPID_vi", "LPID_vi" PID_{vi}^2 = ps \oplus h_1(r.Pub) = PID_{vi}^1 = r.P, PID_vi2 = r.P$. Signature keys are calculated as follows: $LSk_i = s.h_1(TS||PID_vi1||PID_vi2)$. In which TS is a time stamp and r is an integer chosen at random. TA sends OBU a list of pseudonym-IDs and necessary signature keys together with a system parameter so that OBU can produce signatures and verify communications.

4.3. Parameter renewal

When the car's parameters are due to expire, it sends a request to TA to have them renewed. TA produces a new pseudonym and lists of pseudonym IDs and accompanying signature keys with a fresh, brief valid duration after authenticating the request and time stamp. To encrypt the lists, TA uses an elliptic curve to generate symmetric keys that are shared by TA and the cars. In order to decrypt the lists and verify their correctness, the vehicle uses the parameters it received with the new lists to generate symmetric key sharing between the TA and cars. At this stage, the side-channel attack has been thwarted by refreshing the parameters before making them public. Through the 5G-BS node, the vehicle requests the TA renew its parameters. The TA first computes a new set of pseudonym-IDs, such as PID_vi1 and PID_vi2, before using its master key to disclose the original true identity. The vehicle generates a request by computing $sigma_req = h_1(PID_vi_1||PID_vi_2||T_1)$ and sending the resulting tuple to the TA over the 5G-BS. Following are the steps taken by the TA to ensure the accuracy of the timestamp T_1. First, it ensures the accuracy of the time stamp T_1. For each T-second time stamp, the following is verified: so, let's say T is the time lag and T_r is the time of reception. If and only if (T ¿ T_r - T), then T is true. If it doesn't, the message will be discarded. If T_1 holds, then we can move forward. To prevent tampering by a third party, the TA verifies the signature $sigma_req- = sigma_req = h_1(PID_vi1||PID_vi2||T_1)$. TA, meantime, celebrates and double-checks that the registration lists they calculated using the formula $ps = PID_vi2oplush_1(s.PID_vi1)$ were successfully stored. As a result, comparing to RID_v. After issuing a new pseudonym, the TA computes and preloads a new list of pseudonym-IDs and appropriate signature keys to the OBU using the formula $ps_new = h_1(RID_v||s||d_new)$. Pseudonym identifiers are as follows: $PID_vi1 = r_new.P$, $PID_vi2 = ps_new \oplus h_1(r_new.Pub)$, and so on. $LSk_i = s.h_1(PID_vi1||PID_vi2)$ is the formula for the necessary signature keys. In which each of d_new and r_new is an arbitrary positive integer. The TA uses elliptic curve parameters as a shared symmetric key to encrypt a new $LPIDvnew$ and LSk_i. These parameters are then used after being decrypted by vehicle.

4.4. Message signing

At this point, the car uses a pre-sent TA list to pick a pseudonym-ID and signature key at random. The vehicle adds these parameters to the message's signature before broadcasting it. In this stage, an elliptic curve-independent multiplication is utilised instead of a scalar multiplication. To further aid the verifier, a signed vehicle performs a single multiplication operation. Meanwhile, the proposed ES-APP technique utilises the current timestamp for signing messages to prevent replay attacks. The last step is for the vehicle to broadcast a message-signature-tuple containing the signature, the time stamp, and the pseudonym-IDs. The vehicle picks its signature LSk_i and OBU-stored PIDs PID_vi1, PID_vi2 at random. $\sigma_{Msg} = LSk_i.h_1(M||PID_vi1||PID_vi2||T_i)$, where T_i is a timestamp and m is the message exchanged, is signed by the vehicle. To communicate with other cars, it sends out the tuple-based message $\{M, PID^1_{vi}, PID^2_{vi}, T_i, \sigma_{Msg}\}$.

4.5. Single verification

The vehicle sends a message-signature tuple to another vehicle, v_j which verifies the authenticity of the message. The vehicle's data should be verified for validity and freshness using a timestamp before being allowed. The proposed ES-APP approach uses the system's public key to validate the signature and provide proof that the message does not require any tampering from a third party. As a result, the suggested approach will be secure against such assaults. As soon as the tuple-based message $M, PID_vi1, PID_vi2, T_i, sigma_Msg$ was received by the verifying vehicle v_j, the received timestamp T_i was first checked for freshness. The verifier uses the following procedures to examine the signature and the message to ensure its validity and authenticity.

$$\sigma_{Msg}.P =?h_1(PID^1_{vi}||PID^2_{vi}).h_1(M||PID^1_{vi}||PID^2_{vi}||T_i)Pub \quad (1)$$

4.6. Batch verification

Batch verification can be used with the proposed approach. Once the verifier vehicle v_j has received many message-signature tuples from different vehicles, it will evaluate all of them simultaneously using the system's public key. To prevent replay attacks, the proposals update timestamps at this stage. The verifier then uses the public key to ensure that all of these conditions have been met. The following (2) is validated by the vehicle.

$$\sum_{i=1}^{n} \sigma_{Msg}.P =? \sum_{i=1}^{n} h_1(PID^1_{vi}||PID^2_{vi}).h_1(M||PID^1_{vi}||PID^2_{vi}||T_i)Pub \quad (2)$$

5. EXPERIMENTAL RESULTS

In this subsection, the proposed scheme's security is formally verified using the popular automated verification of internet security protocols and applications (AVISPA) simulator to rule out any potential vulnerabilities. We provide implement the proposed scheme and AVISPA results. These two parts are described as follows.

5.1. Implementation the proposed scheme

Since AVISPA is a role-based simulator, players take on specialized roles inside the game. Table 1 explains the details of the AVISPA simulation experiment parameters that were employed. security protocol animator (SPAN) version 1.6 on a computer running Windows 10 Enterprise (64 bit), with support for Ubuntu 10.10 light on virtual machine, an Intel (R) Core (TM) i7-7500U CPU at 2.70 GHz, and 4 GB RAM was used to implement and simulate the presented scheme on AVISPA. Using the Dolev-Yao model with a limited number of sessions, a detected goal, on-the-fly model-checker (OFMC), and a constraint-logic based attack searcher (CL-AtSe) backend, we implemented our proposal scheme taking into account only the vehicle v_i and vehicle v_j. The AVISPA instrument is one of the cutting-edge methods for investigating and analysing protocol safety. To automatically authenticate (by push-button technique) the security properties of the protocols used in server-client/internet of things, this widely used and powerful software solution is indispensable, as shown in Figure 2.

Table 1. AVISPA experiment parameters for computer simulations

Items	Values
Name	SPAN-Ubuntu10.10-light
Platform environment	Ubuntu 10.10 light
Virtual machine	Oracle Virtualbox 7.0.1
RAM	4 GB
SPAN version	1.6
Based CPU	Intel(R) Core(TM)2 Quad 2.66 GHz
Based operation system	Windows 7 Pro
Based RAM	16.00 GB
Based hard disk	145 GB

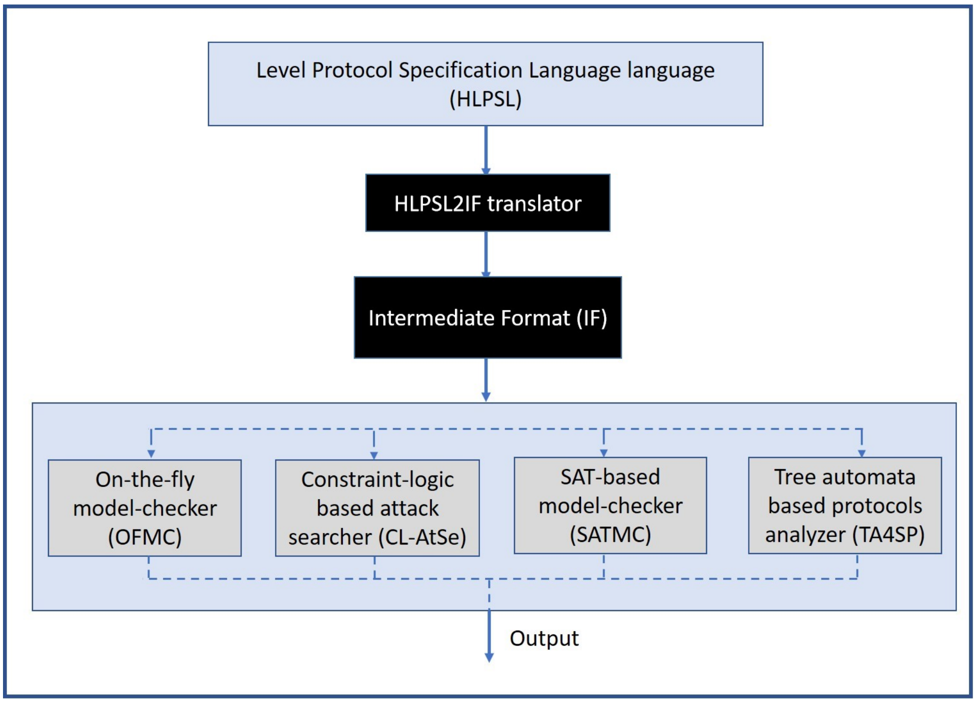

Level Protocol Specification Language language (HLPSL)
HLPSL2IF translator
Intermediate Format (IF)
On-the-fly model-checker (OFMC)
Constraint-logic based attack searcher (CL-AtSe)
SAT-based model-checker (SATMC)
Tree automata based protocols analyzer (TA4SP)
Output

Figure 2. Architecture of AVISPA

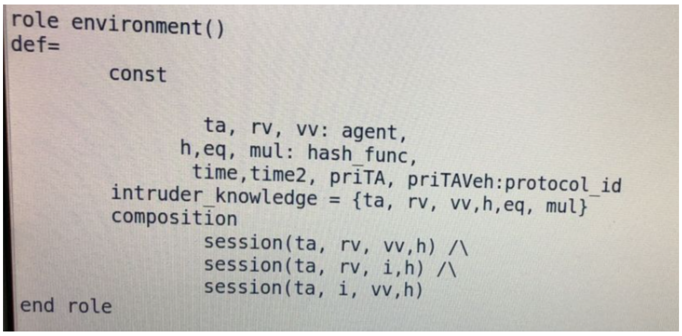
High-level protocol specification language (HLPSL) was used to create the protocol's implementation, and then an HLPSL2IF translator took the protocol's original HLPSL code and translated it into IF [30]–[32]. As for the process of back-ends, it goes as follows: i) on-the-fly model-checker (OFMC), ii) constraint-logic based attack searcher (CL-AtSe), iii) SAT-based model-checker (SATMC), and iv) tree automata based on automatic approximation for the analysis of security protocols (TA4SP). The following are the components of our proposed protocol, which are based on the HLPSL specification:

- Basic role: provides context for the protocol's objects (such vehicle v_i and vehicle v_j).
- Transitions: there must be a statement that includes the beginning as the first basic role. It takes a message being received before this status modifies.
- Composed roles: include one or more fundamental roles for joint execution and designate protocol sessions.
- Environment: includes all sessions; the hacker may pose as a legitimate user in some instances.
- Security goal: specifies the protocol's intended level of protection.

5.2. AVISPA results

This section shows the result of the AVISPA tool. We select two modes of back-end OFMC and ATSE to evaluate the work. The AVISPA tool generates the following sections in its output:

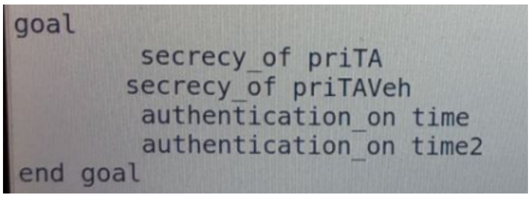
- Summary: it details whether the protocol is secure, risky, or unsure from a security standpoint.
- Details: the output establishes the conditions and setting for evaluating the protocol's claimed safety, lack thereof, or ambiguity, as Figure 3.
- Protocol: here is the name of the protocol that must be followed when keeping records.
- Goal: the protocol's intended level of security is outlined here as Figure 4.
- Backend: one of the four tail tips is shown here.



```
role environment()
def=
        const

                ta, rv, vv: agent,
              h,eq, mul: hash_func,
                time,time2, priTA, priTAVeh:protocol_id
        intruder_knowledge = {ta, rv, vv,h,eq, mul}
        composition
                session(ta, rv, vv,h) /\
                session(ta, rv, i,h) /\
                session(ta, i, vv,h)
end role
```

Figure 3. Environment goal of attack



```
goal
          secrecy_of priTA
         secrecy_of priTAVeh
          authentication_on time
          authentication_on time2
end goal
```

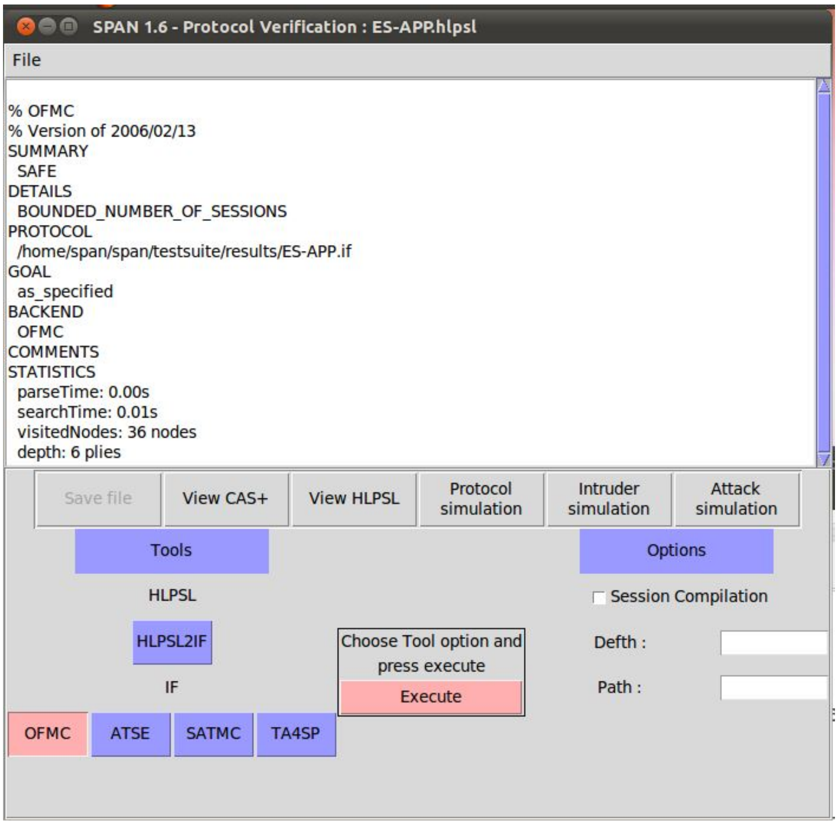
Figure 4. Specified goal of AVISPA

5.2.1. In the case of OFMC

Figure 5 shows the simulated outcomes of the proposed protocol based on OFMC. There were a total of 36 nodes explored, 6 plies were performed, and the search took a total of 0.001 seconds. This finding demonstrates that the proposed protocol is safe against both active and passive attacks as the attacker knowledge in that Figure 3.

5.2.2. In the case of ATSE

Figure 6 shows the simulated outcomes of the proposed protocol based on ATSE. The ATSE protocol analysis concluded that only 45 of the possible 85 states are actually attainable, with a translation time of 0.01 seconds and a computation time of 0.01 seconds. This finding demonstrates that the proposed protocol is safe against both active and passive attacks.



```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/ES-APP.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.01s
 visitedNodes: 36 nodes
 depth: 6 plies
```

Figure 5. Simulated outcomes based on OFMC of proposal

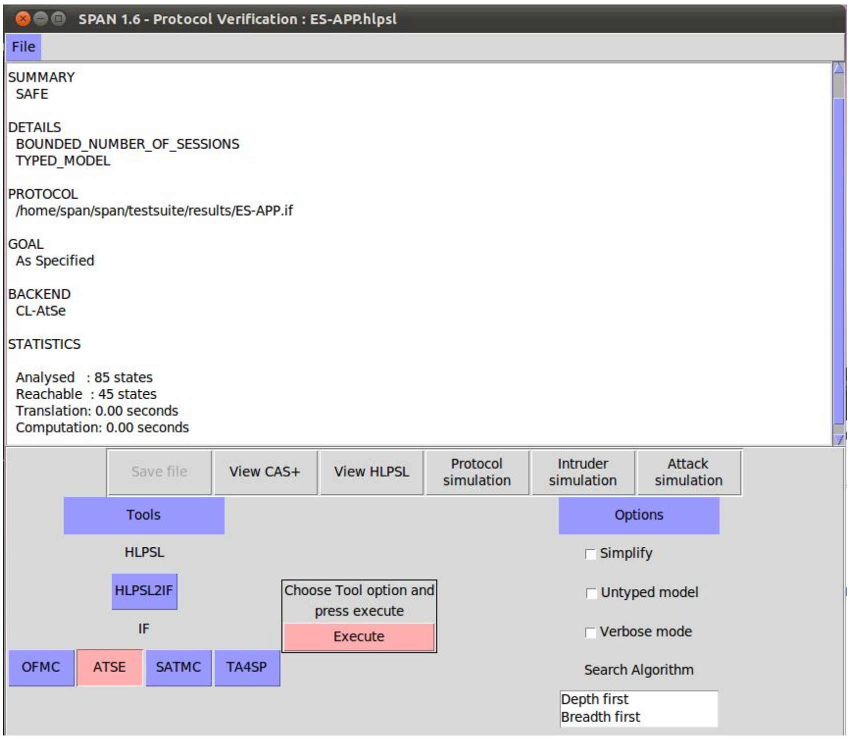
5.3. Dissuasion

Globally, human nature wants to travel to other places or vising friends or achieve their daily activities by using the transportation system such as a car. By increasing road urban and human growth in the world, road accidents and traffic jams have been appearing to damage human live. Annually there are a huge number of people injured or died causes road accidents. Therefore, intelligent transportation systems (ITS) are needed on the road reverent in order to manage and control traffic vehicles.

VANET is a subclass of ITS to reduce road accidents and improve road environment. The main component of the VANETs is TA, RSU, and OBU which interact together. However, since the RSU component is very expensive and compromised any one of them leads to disrupt the system, this work integrates the VANET with 5G technology to be a 5G-enabled vehicle network, as shown in Figure 1. This work uses 5G-BS to communicate vehicles with TA and serve a large number of vehicles during D2D communication. The message exchanged among vehicles are vulnerable to security attacks. The attacker tries to launch malicious activities such as replaying, modifying, and impersonating messages in order to distribute the system. This is because of the nature public environment in vehicular networks. Before deploying the smart system, privacy and security should be condensed by proposing a strong authentication scheme.

There are several researchers that proposed authentication schemes to secure and protect messages shared among vehicles. These schemes use types of security cryptography algorithms to sign messages and verify signatures once obtained before accepting the messages. However, these schemes are huge overhead performance and are valuable to security attacks such as side-channel attacks. As a result, we proposed an ES-

APP scheme that TA, 5G-BS, and OBU are interaction components together. The six steps that make up the proposed ES-APP approach are initialization, vehicle registration, parameter renewal, message signing, single verification, and batch verification. In order to improve the security of the proposed ES-APP scheme, we use the formal evaluation AVISPA tool based on two types of back-ends such as OFMC and ATSE. Figures 5 and 6 show results of AVISPA tool. The ES-APP protocol is shown to be secure against active and passive attacks using the AVISPA tool, as shown in the results section.



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/ES-APP.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 85 states
  Reachable  : 45 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

Figure 6. Simulated outcomes based on ATSE of proposal

6. CONCLUSION

This paper has formally evaluated the proposed authentication (ES-APP) scheme in a 5G-enabled vehicle network using AVISPA. The system model of the proposed consists of three main components in the system. These components are TA, 5G-BS, and OBU. We detail the ES-APP method, a proposed approach to lowering the system's overhead while maintaining security and privacy. The six steps that make up the proposed ES-APP approach are initialization, vehicle registration, parameter renewal, message signing, single verification, and batch verification. The subsequent sections go into detail regarding these phases. Based on the AVISPA tool, the result part proves that the suggested (ES-APP) protocol is secure against any kind of attack, whether active or passive.

REFERENCES

[1] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi, and K. A. Aldhlan, "HAFC: handover authentication scheme based on fog computing for 5G-assisted vehicular blockchain networks," *IEEE Access*, vol. 12, pp. 6251–6261, 2024, doi: 10.1109/ACCESS.2024.3351278.

[2] M. H. Tuama, W. M. Mashloosh, H. M. Albehadili, M. Alazzawi, and M. A. Al-Shareeda, "Beyond polarity: the potential applications and impacts of sentiment analysis and emotion detection," *AlKadhum Journal of Science*, vol. 1, no. 2, pp. 44–51, 2023, doi: 10.61710/akjs.v1i2.51.

[3] M. J. N. Mahi *et al.*, "A review on VANET research: perspective of recent emerging technologies," *IEEE Access*, vol. 10, pp. 65760–65783, 2022, doi: 10.1109/ACCESS.2022.3183605.

[4] M. A. Al-Shareeda and S. Manickam, "A systematic literature review on security of vehicular ad-hoc network (VANET) based on VEINS framework," *IEEE Access*, vol. 11, pp. 46218–46228, 2023, doi: 10.1109/ACCESS.2023.3274774.

[5] M. E. S. Saeed, Q. Y. Liu, G. Tian, B. Gao, and F. Li, "Remote authentication schemes for wireless body area networks based on the internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4926–4944, 2018, doi: 10.1109/JIOT.2018.2876133.

[6] M. A. Al-Shareeda and S. Manickam, "MSR-DoS: modular square root-based scheme to resist denial of service (DoS) attacks in 5G-enabled vehicular networks," *IEEE Access*, vol. 10, pp. 120606–120615, 2022, doi: 10.1109/ACCESS.2022.3222488.

[7] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs)," *Sensors*, vol. 23, no. 5, p. 2594, 2023, doi: 10.3390/s23052594.

[8] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, "L-CPPA: lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system," *PLoS ONE*, vol. 18, no. 10, p. e0292690, 2023, doi: 10.1371/journal.pone.0292690.

[9] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 9, pp. 113226–113238, 2021, doi: 10.1109/ACCESS.2021.3104148.

[10] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G security: a review of design and implementation issues," *Future Generation Computer Systems*, vol. 101, pp. 843–864, 2019, doi: 10.1016/j.future.2019.07.006.

[11] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: an efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *PLoS ONE*, vol. 18, no. 6, p. e0287291, 2023, doi: 10.1371/journal.pone.0287291.

[12] N. Gupta, R. Manaswini, B. Saikrishna, F. Silva, and A. Teles, "Authentication-based secure data dissemination protocol and framework for 5G-enabled VANET," *Future Internet*, vol. 12, no. 4, p. 63, 2020, doi: 10.3390/FI12040063.

[13] B. A. Mohammed *et al.*, "FC-PA: fog computing-based pseudonym authentication scheme in 5G-enabled vehicular networks," *IEEE Access*, vol. 11, pp. 18571–18581, 2023, doi: 10.1109/ACCESS.2023.3247222.

[14] M. Al Shareeda, A. Khalil, and W. Fahs, "Realistic heterogeneous genetic-based RSU placement solution for V2I networks," *International Arab Journal of Information Technology*, vol. 16, no. 3ASpecial Issue, pp. 540–547, 2019.

[15] 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, no. 5, pp. 95–105, 2013, doi: 10.5121/ijnsa.2013.5508.

[16] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, and A. Qtaish, "Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks," *Mathematics*, vol. 11, no. 2, p. 399, 2023, doi: 10.3390/math11020399.

[17] B. Chen, Z. Wang, T. Xiang, J. Yang, D. He, and K. K. R. Choo, "BCGS: blockchain-assisted privacy-preserving cross-domain authentication for VANETs," *Vehicular Communications*, vol. 41, p. 100602, 2023, doi: 10.1016/j.vehcom.2023.100602.

[18] Z. G. Al-Mekhlafi *et al.*, "Efficient authentication scheme for 5G-enabled vehicular networks using fog computing," *Sensors*, vol. 23, no. 7, p. 3543, 2023, doi: 10.3390/s23073543.

[19] J. Zhang, H. Fang, H. Zhong, J. Cui, and D. He, "Blockchain-assisted privacy-preserving traffic route management scheme for fog-based vehicular ad-hoc networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2854–2868, 2023, doi: 10.1109/TNSM.2023.3238307.

[20] A. A. Almazroi, M. H. Alkinani, M. A. Al-Shareeda, and S. Manickam, "A novel DDoS mitigation strategy in 5G-based vehicular networks using chebyshev polynomials," *Arabian Journal for Science and Engineering*, pp. 1–14, Dec. 2023, doi: 10.1007/s13369-023-08535-9.

[21] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-fog: a novel anonymous authentication scheme for 5G-enabled vehicular fog computing," *Mathematics*, vol. 11, no. 6, p. 1446, 2023, doi: 10.3390/math11061446.

[22] M. A. Alazzawi, H. A. H. Al-Behadili, M. N. S. Almalki, A. L. Challoob, and M. A. Al-Shareeda, "ID-PPA: robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network," *Communications in Computer and Information Science*, vol. 1347, pp. 80–94, 2021, doi: 10.1007/978-981-33-6835-4_6.

[23] Z. G. Al-Mekhlafi *et al.*, "Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks," *Electronics (Switzerland)*, vol. 12, no. 4, p. 872, 2023, doi: 10.3390/electronics12040872.

[24] M. Bayat, M. Barmshoory, S. M. Pournaghi, M. Rahimi, Y. Farjami, and M. R. Aref, "A new and efficient authentication scheme for vehicular ad hoc networks," *Journal of Intelligent Transportation Systems: Technology, Planning, and Operations*, vol. 24, no. 2, pp. 171–183, 2020, doi: 10.1080/15472450.2019.1625042.

[25] M. A. Al-Shareeda and S. Manickam, "COVID-19 vehicle based on an efficient mutual authentication scheme for 5G-enabled vehicular fog computing," *International Journal of Environmental Research and Public Health*, vol. 19, no. 23, p. 15618, 2022, doi: 10.3390/ijerph192315618.

[26] U. Bansal, J. Kar, I. Ali, and K. Naik, "ID-CEPPA: identity-based computationally efficient privacy-preserving authentication scheme for vehicle-to-vehicle communications," *Journal of Systems Architecture*, vol. 123, p. 102387, 2022, doi: 10.1016/j.sysarc.2021.102387.

[27] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "SE-CPPA: a secure and efficient conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *Sensors*, vol. 21, no. 24, p. 8206, 2021, doi: 10.3390/s21248206.

[28] J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, "A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography," *IEEE Access*, vol. 9, pp. 15633–15642, 2021, doi: 10.1109/ACCESS.2021.3053043.

[29] M. A. Al-Shareeda *et al.*, "Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU)," *Sustainability (Switzerland)*, vol. 14, no. 16, p. 9961, 2022, doi: 10.3390/su14169961.

[30] T. A. Team, "HLPSL tutorial," *www.avispa-project.org*, 2006. https://www.avispa-project.org/package/tutorial.pdf (accessed Jun. 17, 2023).

[31] A. Armando *et al.*, "The AVISPA tool for the automated validation of internet security protocols and applications," *Lecture Notes in Computer Science*, vol. 3576, pp. 281–285, 2005, doi: 10.1007/11513988_27.

[32] T. A. Team, "AVISPA v1.0 user manual 2006," *www.avispa-project.org*, 2006. https://www.avispa-project.org/package/user-manual.pdf (accessed Jun. 17, 2023).

BIOGRAPHIES OF AUTHORS

Mays A. Hamdan received her bachelor's degree from Diyala University, Iraq in 2013 and Master's degree from Modern University for Business and Sciences, Lebanon in 2020 and is currently studying for her Ph.D. degree in National School of Electronics and Telecommunications of Sfax, University of Sfax. Her research interests include security and privacy issues in VANETs. She can be contacted at email: maysmubs@gmail.com.

Amel Meddeb Maklouf received the Ph.D. degree from SUP'COM, Tunisia, in 2010, and the Habilitation degree, in December 2020. From 2001 to 2004, she worked as the Chief of the Certification Unit, NDCA. Since September 2010, she has been working as an Assistant Professor at ENET'COM, Sfax, Tunisia. Since 2020, she has been the Head of the Telecommunication Department. She was a supervisor of more than 30 master's projects and 14 Ph.D. She co-authored more than 40 papers, published in international journals and refereed conferences. Her research interests include security of vehicular networks, cloud networks, and BSN. She can be contacted at email: amel.makhlouf@enetcom.usf.tn.

Hassene Mnif was born in Sfax, Tunisia, in 1975. He received the Engineer and Master Diplomas in Electrical Engineering from the University of Sfax (ENIS) in 1999 and 2000, respectively, the Ph.D. degree in electronics from the University of Bordeaux I, France, in 2004 and the HDR degree from the University of Sfax in 2011. He is currently full Professor and the President of the Ph.D. Committee in the National School of Electronics and Telecommunications of Sfax, University of Sfax. He was the Director of this school between 2014 and 2020, where he has multiple innovative engineering education initiatives. He is a member of the Electronic and Information Technology Laboratory. His research interests include Energy Harvesting, Design of Radio-frequency integrated circuits, characterization, and compact modeling of both high frequency devices and future emerging technologies like Carbon Nanotube Field Effect Transistor (CNTFET). He also participates in research for real time image and video text extraction and micro mobility systems. He has authored and co-authored about 90 journal publications and conference papers and has gathered significant scientific coordination experience within national and international collaborative research projects. He participated in the organization of several IEEE conferences and workshops, in particular ICECS 2009 and MELECON 2012. He served as the Tunisia Section treasurer between 2011 and 2013, he is actually the IEEE Tunisia Section Chair-Elect. He can be contacted at email: hassene.mnif@ieee.org.