Egyptian Informatics Journal 23 (2022) 83–93

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Authentication scheme for Unmanned Aerial Vehicles based Internet of Vehicles networks

Kashif Naseer Qureshi [a], Muhammad Arslan Saleem Sandila [a], Ibrahim Tariq Javed [b], Tiziana Margaria [c], Laeeq Aslam [d]

[a] Department of Computer Science, Bahria University, Islamabad, Pakistan
[b] Lero-The Irish Software Research Centre, University of Limerick, Limerick V94 T9PX, Ireland
[c] Lero –Science Foundation Ireland Research Centre for Software, University of Limerick, V94 T9PX Limerick, Ireland
[d] Punjab University College of Information Technology (PUCIT), University of the Punjab, 54000, Lahore, Pakistan

ARTICLE INFO

Article history:
Received 26 March 2021
Revised 19 June 2021
Accepted 3 July 2021
Available online 29 July 2021

Keywords:
UAV
IoV
Network
Security
Authentication
Privacy
RSU
Attack
Safety

ABSTRACT

New and advanced technologies have introduced amazing areas like the Internet of Vehicles (IoV) and Unmanned Aerial Vehicle (UAV). These two technologies are emerged to facilitate the ground users by providing more fast and convenient data communication services. Due to the open nature of these networks, security and user privacy is always a serious concern. Different types of security attacks have been noticed in these networks like jamming attacks, global positioning system jamming, signal jamming, and data jamming. The existing solutions have been designed to resolve and tackle security issues such as authenticity, insurance of data integrity, provision of correct message authentication, and removal of redundant authentication. However, existing schemes have some limitations in terms of computational costs and efficiency and do not provide security at all levels. This paper proposes an Efficient Authentication Scheme for Safety Applications for Internet of Vehicles (EASSAIV) for message authentication. The proposed scheme can gather, process, and verify the information delivered to roadside units, UAVs, or to the vehicles and authenticate the received messages. Proposed scheme achieved better performance as compared to state of the art scheme in terms of safety, packet loss, delay and computational cost.

© 2022 Published by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

Internet of Vehicles (IoV) is deemed as a promising research field with huge potential of benefits. It shall streamline global traveling practices. The IoV is a network of internet-connected vehicles with a fleet of sensors installed onboard to gather process and forward the data for further decision [1–3]. The IoV is based on advanced technologies including Internet, cloud, and edge, fast 5G services where the information is disseminated over the Internet by nearby vehicles, pedestrians via handheld devices, roadside infrastructure, and other transport management systems [4]. Consequently, IoV enabled environment ensures a better traveling experience with safe navigation and road safety. However, challenges in the implementation of IoVs remain with routing resource allocation, disruption/disconnection of network services, processing of big data, message authentication, broadcast of the secure channel, and high-cost impact. To facilitate the IoV network, the Unmanned Aerial Vehicle (UAV) has introduced which are drones or aircrafts used for private and public applications [5,6]. Drone communication services can be used for different purposes such as delivery, monitoring, military usage for security [4,7]. To control the drones, some interfaces are used like the computer, remote control, smart devices, and other software applications [8–10]. The updates among nodes are initiated by using a short beacon or Hello messages which are periodically broadcasted in the networks and the network suffered from high overhead [11]. Routing is the main factor of communication between the UAVs and the IoV network which provides the communication services. The integration of UAV technology with IoV technology has presented several routing and security challenges [12].

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

E-mail addresses: knaseer.buic@bahria.edu.pk (K.N. Qureshi), arslansandila@gmail.com (M.A.S. Sandila), Ibrahimtariq.javed@lero.ie (I.T. Javed), Tiziana.Margaria@lero.ie (T. Margaria), laeeq.aslam@pucit.edu.pk (L. Aslam)

https://doi.org/10.1016/j.eij.2021.07.001
1110-8665/© 2022 Published by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Ensuring security and maintaining privacy at the same time is an additional challenge that needs to be addressed alongside issues related to mobility and reliability. Lack of open standards for intra-vehicle communication and interoperability is a big hurdle in accelerating adoption [1,13]. Some of the major challenges in UAV-based IoV networks are privacy, real-time response, dynamic support, data validation, and jamming [11,14]. Privacy is undoubtedly being one of the prime concerns, to accurately determine different situations like an accident, the vehicle needs to accurately report its identity to the UAV but this identity can be used/exploited by unwanted users. Accurate validation of data is very important as it can play a crucial role in keeping roadside units away from garbage data processing and flooding of spam messages. IoV is also prone to jamming attacks e.g. GPS jamming, signal jamming, and even data jamming. These attacks can lead to the collapse of the whole concept of autonomous vehicles. Researchers divided these threats into inter-vehicle security threats and intra-vehicle security threats. Researchers also explained different types of attacks that can encounter ranging from the physical layer up to the application layer. These attacks include Illusion and GPS spoofing attacks using sensor tempering. This attack results in providing false information to the On-Board Units (OBU) of the vehicle by compromising the sensors. Consequently, resulting in the broadcasting of wrong information into the network regarding different measurements of the vehicle including speed and location, and ultimately results in creating the illusion of incidents that have not happened. In addition to this, other attacks that need sheer focus to be resolved include Denial of Service (DoS) attack in which resources are being choked to provide services, Sybil attack is used to send incorrect information about traffic congestion and road conditions, replay attack enables retransmission of the previous message to create confusion, black hole attack, and passive eavesdropping attack [15,16]. Fig. 1 shows the complete architecture for the UAV-based IoV networks.

To cater to all such issues, researchers have provided a lot of solutions to deal with message authentication. In a study [17], researchers proposed an efficient authentication scheme that deals with problems associated with certificate distribution and certificate revocation list CRLs. Primarily in pseudonym and group-based message authentication schemes, vehicles need to store a valid certificate generated by the management center and before message authentication, the receiver has to check the CRL. These CRLs have data in bulk and require heavy computational resources and storage capacity. Additionally, the Trusted Authority (TA) involvement fails in such schemes in the real-world. Subsequently, the scheme proposed in this study is using the certificate-less signature in a semi-trusted authority environment with a self-healing key distribution method. This enables the receiver to authenticate the message without the need to query the CRL. In this way, storage space and communication resources are saved thus increasing the efficiency of message authentication. The IoV applications and different security threats that might come across Vehicular Ad Hoc Networks (VANETs) implementation and thoroughly deliberate that existing security solutions use conventional cryptographic techniques. Most of these require high bandwidths and ultra-fast networks, so this study proposed a lightweight authentication protocol based on Radio-Frequency Identification Devices (RFID) [18]. The existing solutions are designed to resolve different problems such as reduction of time and cost, genuine authenticity, insurance of data integrity, provision of correct message authentication, and removal of chances for redundant authentication, and so on. However, existing schemes have some limitations concerning computational costs and efficiency and these do not provide security at all levels. Hence, the proposed Efficient Authentication Scheme for Safety Applications for Internet of Vehicles (EASSAIV) scheme explicitly focused on safety applications for UAV-based IoV networks to overcome the authenticity issues. The main objectives of this paper are as follows:

- Design a scheme that can quickly gather, process, and verify the information delivered to RSU, UAV, or vehicles to authenticate the received messages.
- Proposed scheme tackles the authenticity, insurance of data integrity, provision of correct message authentication, and removal of redundant authentication.

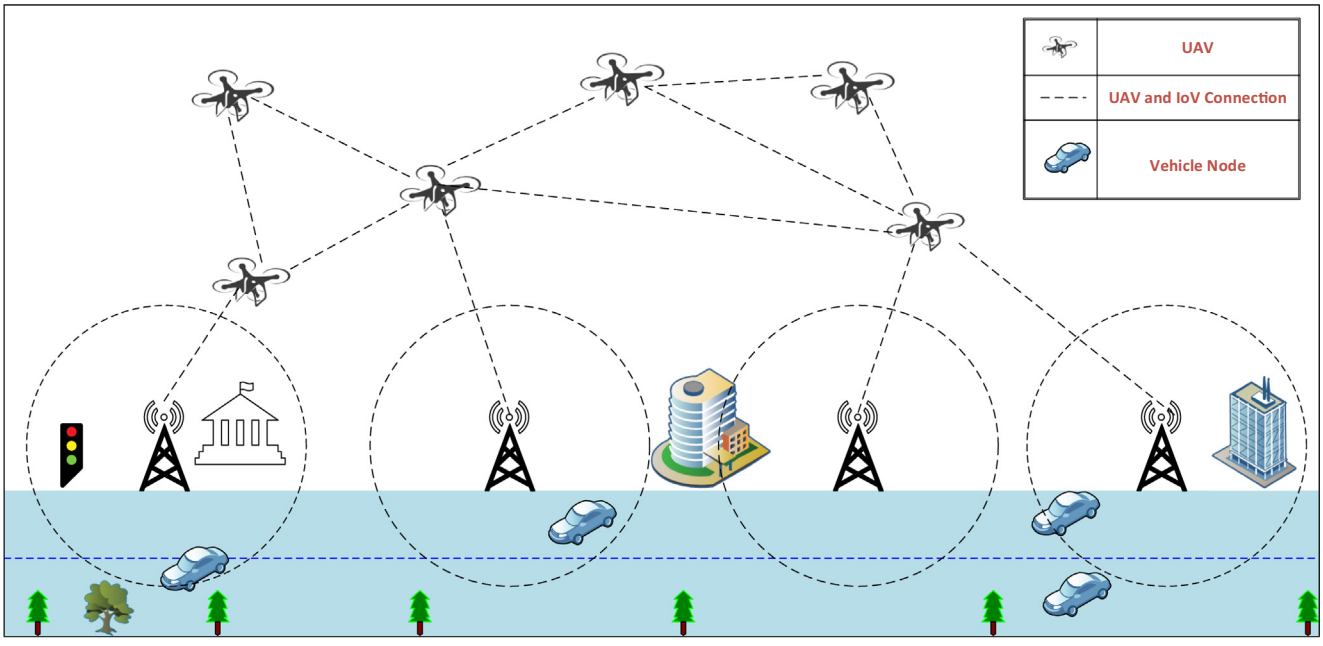


Fig. 1. UAV-based IoV Network.

- Proposed scheme validates in security tool to check the safety and working process scenically in safety applications concerning UAV-based IoV and to decrease the overheads in the network.

This paper is organized as follows: Section 2 presents the overview of related studies and research articles, which are related to the proposed research work. Section 3 explains the proposed mechanism in detail with all its working, security model, and authentication protocol. Section 4 presents the results, analysis. The last section concludes the paper with future direction.

2. Related work

In [19], authors proposed a Secure Authentication Scheme for VANETs with Batch Verification (SAS-VANET) based on three phases including key generation and pre-distribution, pseudo-identity generation and message signing, message verification. The first phase uses system parameters for the vehicles and RSUs. In the second phase, the vehicle uses its unique identity and runs the pseudo-identity generation process. In the last phase, the message is verified and accepted. The RSU is also verifying the message by using batch verification. The proposed scheme is evaluated in terms of average delay and lost packet rate. The results indicated the better performance of the proposed scheme is compared to the previous scheme. However, this scheme is not feasible for high mobility nodes and dynamic topological changes like in vehicular ad hoc networks.

In [20], the authors explained the infrastructure authentication scheme and discussed two types of infrastructure elements. OBUs are mounted on vehicles, and Road Side Units (RSUs) are deployed at the roadside as an infrastructure. These infrastructures communicate usually with the help of the TA for the integration of registration and provision of authentication services. The proposed scheme consists of four phases including system initialization, key generation, signing stage, and verification stage, and then these phases are technically explained. Afterward, the security analysis is conducted and lastly, performance evaluation is done. Authors claimed that results where the proposed scheme contained costs 1.050 ms and 3.683 ms in terms of signing and verification respectively. In this scheme, the helper is assumed as a fully trusted device and the private key of the vehicle is generated by its helper. Subsequently, this work is extendable, and designing an efficient threshold key insulated authentication scheme is the way forward which aims to achieve feasible secure V2I communication. However, this work is based on assumption where authors discussed that all devices are trustworthy and private key generated by its helper. Usually this phenomenon is not well suited for high mobility based and open networks.

In [21], the authors proposed a privacy-preserving sensory data sharing scheme and addressed location privacy preservation, sensory data acquisition, and collection issues of IoV networks. This data collection and distribution is collected by sensor nodes and onboard devices installed in vehicles. Researchers modified the pallier cryptosystem with the structuring of multi-dimensional sensory data that is recorded at different locations. The modified pallier cryptosystem helps in achieving privacy-preserving sensory data aggregation for location. In the second phase, data acquisition is performed. In this phase, the proxy re-encryption technique is used to achieve results related to location privacy preservation of data querying at the network edge. This implies location privacy preservation without the involvement of a trusted central entity. It is expressed that during data aggregation, the location-based data queries may violate the location privacy of vehicles. Existing schemes are mostly designed for cloud environments that are outsourced with typically fixed storage. The proposed scheme also maintains data integrity and collision attack resistance. The results showed that the proposed scheme largely reduced the computational overhead and communication cost in comparison with existing OT and data aggregation protocols. However, vehicle nodes mobility is one of the important factor to design any kind of security solution for IoV network.

In [22], the authors discussed routing, quality of service, broadcasting, and security in issues for vehicular ad hoc networks. These networks have life-threatening and life-crucial scenarios therefore security being the primary most factor and need top priority. Therefore, this paper discusses different possible attacks including DoS, broadcast tempering, malware spamming, and black hole attacks. Similarly, the authors discussed threats involved in authenticity, this includes threats about message or identity masquerading, replay attacks, and GPS spoofing. The authors pointed out tunneling, position faking, and message tampering as potential threats that can hamper authenticity. Subsequently, message suppression and key/certificate replication are also discussed. However, this type of solutions suffered with real-time constraint, and limited computing resources.

In [23], authors discussed an efficient message authentication with revocation transparency using Blockchain for vehicular networks to address the main concerning issues of security and privacy. The proposed scheme is based on pairing-free online/offline certificate with less signature with efficient revocation. The authors used the cuckoo filter to enhance efficiency, this allows RSUs to assist nearby vehicles in the verification of signatures. The proposed study enlightens the revocation handling by key generation center updating time keys of non-revoked users. A node selection algorithm is used for the reduction of the workload of the key generation center. This paper uses Blockchain technology to store the revocation list. This strategy enhanced the transparency of user revocation where vehicles are independent to check the revocation lists from validated Blockchain concept. Subsequently, an efficient signature scheme is proposed with pairing a free certificate online/offline system. The complexity is logarithmic to the number of users and conducted through a public channel. Lastly, the authors conducted security and efficiency analysis, and a comparison with existing solutions where the proposed signature scheme meets all the security and privacy requirements of vehicular networks. However, the workload of the key generation centre, and verification of certificates consumed more resources and computational power.

In another study [24], the authors discussed secure authentication and privacy-preserving techniques in vehicular ad hoc networks. The authors explained that the privacy of vehicles should be maintained by keeping the vehicle's identity and location information. But along with privacy, the message sent from the vehicle needs to be verified and no one except relevant authorities should be able to determine the identity or location of the vehicle from the message from the vehicle. Authentication is divided into two parts including node authentication and message authentication. This research promises to fill the gap created in the last decade and protocols discussed in the research paper are classified into different categories based on the problems addressed as well as tools and techniques used to provide solutions. The authors claimed that this work would also serve as a suitable reference for researchers working on privacy, authentication, and secure message dissemination in VANETs. However, this study still suffered with privacy, and secure message dissemination issues.

In [25], the authors discussed an enhanced anonymity resilience security protocol for vehicular ad hoc networks. This work is an enhancement and refinement of an earlier proposed protocol. The authors proposed a robust protocol that ensures security protection on existing security attacks. Also, it protects all related

possible attacks. The authors also performed simulations through Scyther and confirm that all the private information is protected while developing the common key. The proposed solution has five distinct phases including system setup, user registration, system login, mutual authentication, and data authentication. Subsequently, formal security verification is done using a broadly accepted Scyther tool. It is to formally analyze security protocols and potential vulnerabilities. The results show better performance in terms of computation and communication overheads. However, road safety measures, multimedia data transfer, and vehicle performance data are some important factors which need attention.

Many researchers have been proposed various authentication models involving different cryptographic techniques including Elliptic Curve Cryptography. Where these schemes may fulfill the purpose to some extent, on the other hand, they are not meaningful in the real-time scenario as of IoV limitations of fast-moving vehicles and very little time available for authentication and validation. The idea of smooth implementation of UAV-based IoV is not simple as it comes with a lot of constraints that possess serious life threats if not handled properly. Different studies concerning message authentication are thoroughly deliberated and grey areas are figured out [26,27]. These involve the high computational costs, communication overheads, redundant authentication, false authentication, prone to attack authentications, eavesdropping, and timely authentication failures. After studying deeper, it is revealed that research done in message authentication for explicit safety applications is very limited thus requires to be explored more. This research is focused on an efficient message authentication scheme for safety applications for UAV-based IoV. Table 1 shows the existing studies comparison.

3. Proposed scheme

The UAV-based IoV networks are using communication between different vehicle nodes and drones where message authentication is a core factor for security provision. This communication process involves several phases including the authentication phase, key exchange phase, and the data transfer phase. Several message authentication schemes have been introduced to overcome these issues but most of these schemes suffer in the provision of complete security at all stages of message authentication. To address the aforementioned issues in this research, an Efficient EASSAIV is proposed. This proposed scheme secures the information between the imparting vehicles utilizing asymmetric encryption procedures for example using the public key and private key encryption and decoding. This encryption-decoding measure is utilized to trade information between the vehicles and with drones securely. The proposed scheme is based on three main phases including the initial deployment phase, implementation phase, and operational phase. The first phase is relatively brief and the latter two phases are more comprehensive. These phases are the core of the entire model and the complete concept is explained thoroughly in these phases.

3.1. Initial deployment phase

The initial deployment phase initiates at the manufacturer's site before the vehicles are shipped to the owner. In this phase, the manufacturer shall preinstall these vehicles with requisite data and cryptographic subtleties relating to correspondence/association with the cloud server. This makes a believed correspondence connect between the manufacturer and vehicles. All onboard sensors are also equipped into vehicles during this phase. This shall also be useful to execute remote procedures like updating new software patches or downloading the new and latest version of firmware in vehicles without the requirement of bringing the vehicles to some service center physically. Also, every vehicle is equipped with a personal user device for the owner of the vehicle for the establishment of communication between vehicles and gateway. This also serves as an extra layer of security and prevents unauthorized access of the vehicle to the gateway. The controller in the distant server produces the vehicle identification, $ID_{1,}$ and utilizing an RNG, it figures the vehicle's private and public key. It likewise produces a one-time access secret key or password (OT). The one time secret key or password provides a mechanism for logging on to the network or service using unique password which is used once. This method prevents the second time usage of vehicle password and ensures strong authentication mechanism. These public and private keys of vehicle V_1, the vehicle's ID worth, and access secret key are stacked into the vehicle's memory over a protected

Table 1
Existing Studies Comparison.

Proposed Scheme	Technique & Remarks	Performance	Limitations
Secure Authentication Scheme for VANETs with Batch Verification (SAS-VANET) [19]	Uses key generation and pre-distribution, pseudo-identity generation and message signing, message verification	Better in term of average delay, and lost packet rate	Dynamic topologies and high mobility are not considered.
An Efficient V2I Authentication Scheme for VANETs [20]	An efficient vehicle to infrastructure authentication scheme specific for VANETs. It is explained that in vehicular ad hoc networks.	The performance evaluation shows the proposed scheme costs 1.050 ms and 3.683 ms in terms of signing and verification respectively.	Dynamic topologies and high mobility are not considered.
A privacy-preserving sensory data sharing scheme [21]	This scheme is used for data sharing with collision resistance in IoV networks for data collection and distribution.	This scheme enhanced and validated the security properties and improve the computation and communication efficiency	Vehicle nodes mobility is not considered
Edge computing-based Security and Privacy Scheme [22]	A novel edge computing-based message authentication scheme. It can serve multiple mobile devices in intelligent connected vehicles.	The secure scheme in the random oracle model and can resist two types of adversaries under certificate less public key encryption.	Real-time constraint, limited computing resources
Efficient Message Authentication with Revocation Transparency Using Blockchain for Vehicular Networks [23]	An efficient message authentication with revocation transparency using Blockchain for vehicular networks to address the main concerning issues of security and privacy.	Analysis of revocable signature scheme by comparison of computation time and signature size of the proposed scheme with existing schemes results in better performance.	The workload of the key generation center, verification of certificates.
Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs) [24]	A thorough and well-deliberated Review on Secure authentication and privacy-preserving techniques of last decade in vehicular ad hoc networks.	A comparative analysis is done on basis of different classifications of papers.	Privacy, Authentication, Secure Message Dissemination.
An enhanced anonymity resilience security protocol [25]	An enhanced anonymity resilience security protocol for the vehicular ad hoc networks. This work is an enhancement and refinement of an earlier proposed protocol.	Scyther is used to perform simulations to confirm all private information protection during the establishment of the common key.	Road safety measures, Multimedia data transfer, Vehicle performance data.

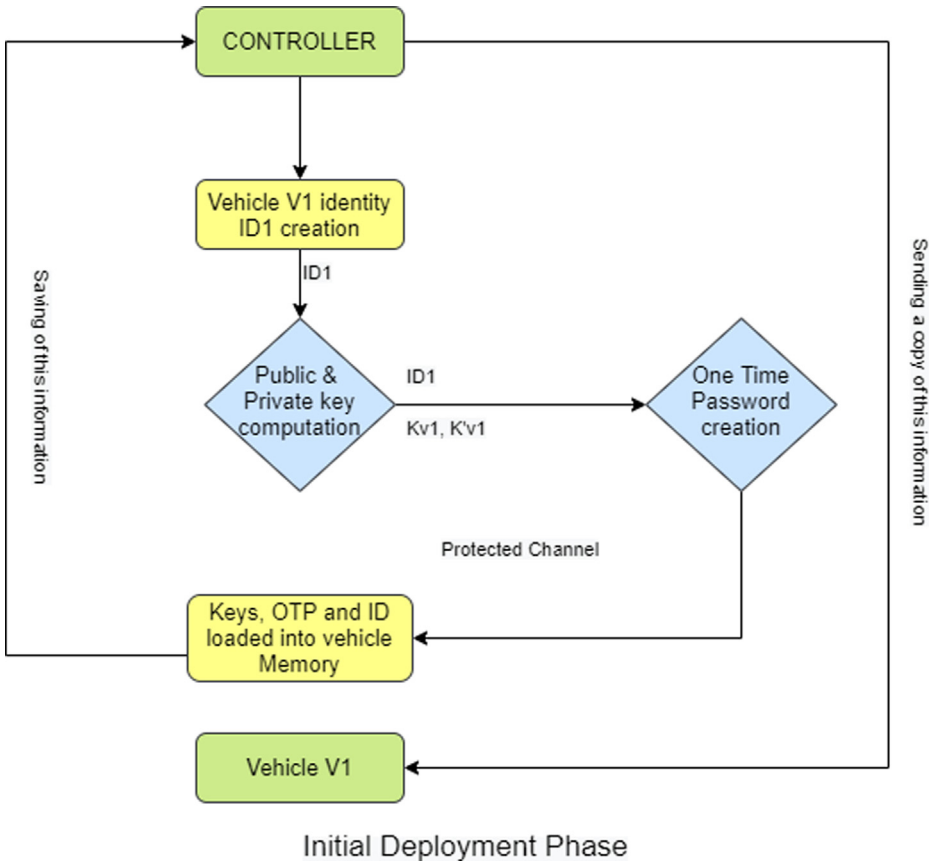


Fig. 2. Initial Deployment Phase.

channel, for example, one that is impervious to altering and catching, accomplished through the cryptographic conventions executed by the maker. The regulator in the distant worker spares these in its information base and sends the vehicle *ID*, ID_1, and the one-time access secret word, P_1 to the vehicle V_1 as shown in Equation 1:

$$C \rightarrow V_1 : En\ \{ID_1,\ P_1,\ K_{v1},\ K'_{v1}\} \quad (1)$$

*where En{} implies encryption of data inside the supports as shows in Fig. 2.

Fig. 2 shows the initial deployment phase.

3.2. Implementation phase

At this point when the owner gets the IoV vehicle, $\boldsymbol{V_1}$, a solicitation for verification data from the cloud server is produced with the goal that the holder can get to the sensors installed vehicle. The cloud server's controller sends the holder One Time Password (OTP), which when gone into the IoV $\boldsymbol{V_1}$, will give the holder admittance to it and its administrations. Fig. 3 shows the implementation phase.

When the owner accesses IoV V_1, the vehicle can associate with the network server through smart gateway *G*. The owner's device (accompanied by vehicle by the maker) sends the identity of the

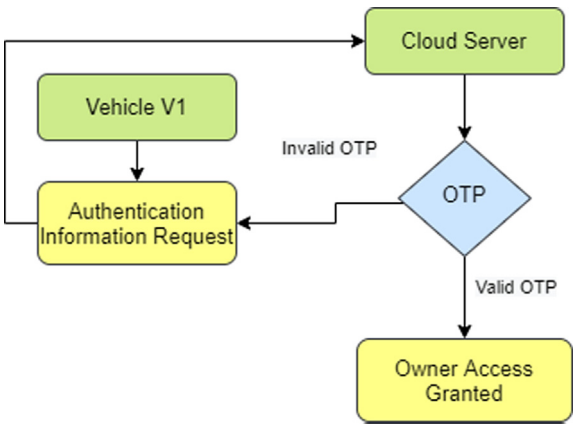


Fig. 3. Implementation Phase.

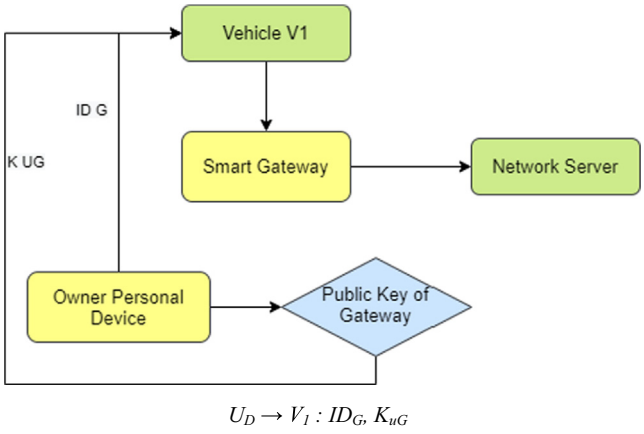
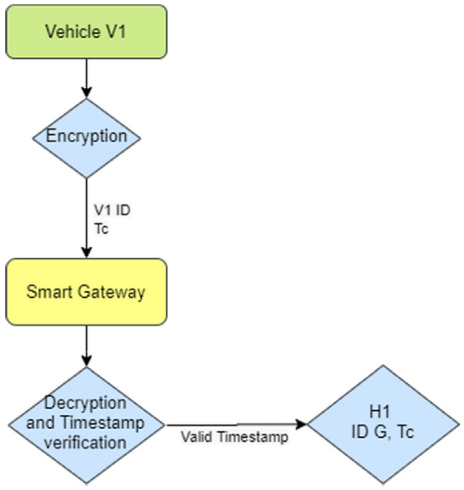


Fig. 4. Public Key Exchange.



$V_1 \rightarrow G : \{T_c\}\, K_{uG}, \{ID_1\}\, H_1(ID_G, T_c)$

*where T_c is the current timestamp

Fig. 5. Encryption Process.

smart gateway, ID_G, and its public key, K'_{uG}, to V_1. Fig. 4 shows the public key exchange process.

$U_D \rightarrow V_1 : ID_G,\ K_{uG}$

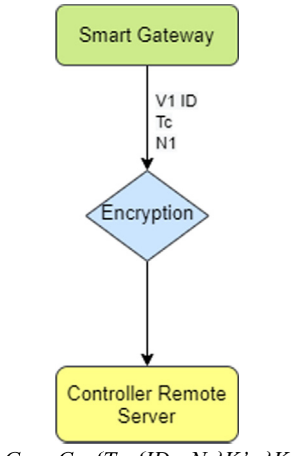
The vehicle, V_1, scrambles and sends to the gateway its ID alongside the current timestamp to the smart passage to be enlisted in the system. On accepting the information from V1, the passage will unscramble the collected message and check the timestamp. If authentic, it will enumerate H_1 (ID_G, T_c) which was the encryption key used to encrypt the ID of V_1. Fig. 5 shows the encryption process.

$V_1 \rightarrow G : \{T_c\}\ K_{uG},\ \{ID_1\}\ H_1(ID_G,\ T_c)$

*where T_c is the current timestamp

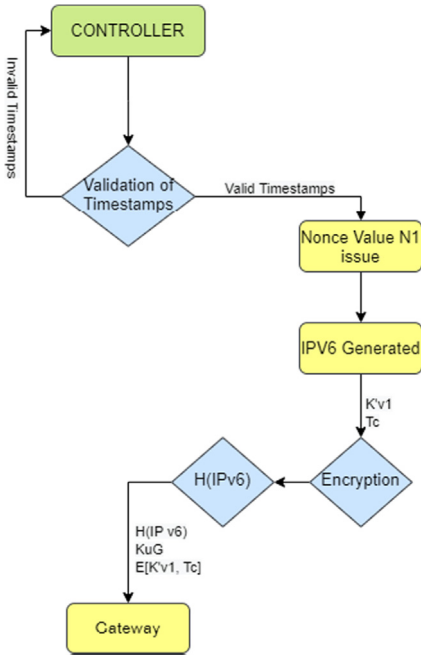
Once only the gateway accesses the vehicle identification proof, it advances three limitations to the regulator in the remote server for example the vehicle character, the current timestamp, and a nonce N1, all scrambled properly as appeared in the condition beneath. Fig. 6 shows the encryption process on the gateway side.

$G \rightarrow C : \{T_c,\ \{ID_1,\ N_1\}K'_{uc}\}K_{uc}$



$G \rightarrow C : \{T_c, \{ID_1, N_1\}K'_{uc}\}K_{uc}$

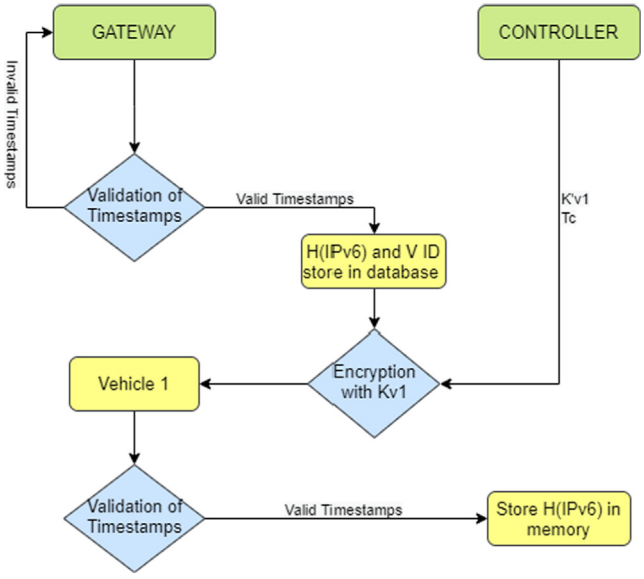
Fig. 6. Encryption Process.



$C \rightarrow G : H(IP_{v6}), \{\{\ K_{uG}\}\, K'_{v1},\ T_c\}\, K_{uG}$

Fig. 7. Gateway Authentication Timestamp Process.

The timestamp expresses facts about the occurring of an event, on the other hand, the nonce is an assessment value that is utilized just a single time and is utilized to recognize one case of the protocol from the other. The selection of nonce value and timestamps also helps in the provision of deterrence against a replay attack. The controller ensures if the nonce value is not issued prior, it is done by comparing and validating the received timestamp with the current timestamp. The vehicle ID is obtained and the controller creates a virtual identity for V_1 and stores the ID in the database. The controller now sends the concatenated values of the virtual identity of V_1, and encrypted values of Vehicle V_1 private



$G \rightarrow V_1 : H(IP_{v6}), \{\{\ K_{uG}\}\ K'v1,\ T_c\}\, K_{v1}$

Fig. 8. Gateway and Controller Process.

key with Gateway G public key along with a current timestamp and send it to the gateway. Fig. 7 shows the gateway authentication timestamp process.

$$C \rightarrow G : H(IP_{v6}), \{\{K_{uG}\}K'_{v1}, T_c\}K_{uG}$$

After performing this, the gateway authenticates the timestamp and saves the hash of virtual identity IP_{v6} along with the respective vehicle ID in the database. Now the gateway shall forward the hash value and its public key encrypted with the vehicle's private key that is received from the controller and timestamp. Fig. 8 shows the gateway and controller process. This complete information is then encrypted by Vehicle 1 private key. V_1 now checks the timestamp and upon validation, the hash value is stored in the memory of V_1 as follows:

$$G \rightarrow V_1 : H(IP_{v6}), \{\{K_{uG}\}K'_{v1}, T_c\}K_{v1}$$

The gateway and controller process is proposed in this research based on the concept of having its local database. This database is utilized by all the vehicles in the network to access the requisite information. The network also uses the gateway database when required. The gateway is also responsible for communication with roadside infrastructure. The information stored in the database of the gateway is uploaded and updated to the cloud server periodically. The cloud server has information regarding all networks and all vehicles that are connected with these networks. Instead, the gateway only has information about the vehicles connected within its network.

3.3. Operational phase

The operation phase of this proposed scheme explains the basis of vehicle-to-vehicle communication during the regular working of vehicles within a network. If a vehicle V_1 wants communication to another vehicle V_2 to perform some task, V_1 needs to forward a request to the gateway first by sending information like hash value, current timestamp, and V_1 own public key. Fig. 9 shows the vehicle and gateway process.

$$V_1 \rightarrow G : H(IP_{v6}), \{T_c, V_2\}K_{uG}$$

Validation of timestamp is performed by the gateway; upon successful validation, the gateway checks its database for information about V_2. After this gateway sends K_{12} to Vehicle 1. This is a shared key for establishing communication between Vehicle 1 and Vehicle 2. Along with the shared key, the gateway sends a second nonce value N_2 after concatenation with the current timestamp. The gateway public key K_{uG} is concatenated with shared key K_{12}. Now the gateway performs encryption by vehicle 2 private key and vehicle 1 public key. Fig. 10 shows the complete process.

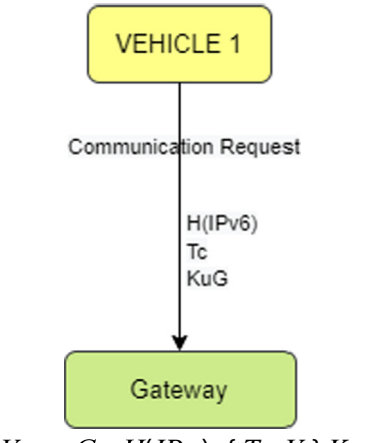


Fig. 9. Vehicle and Gateway Process.

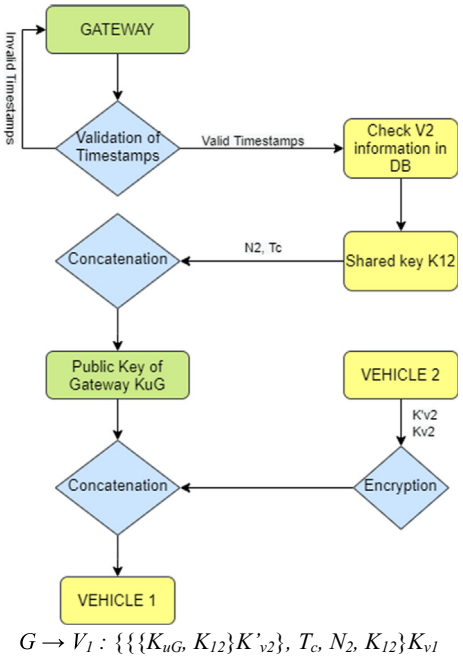


Fig. 10. Complete Process.

$$G \rightarrow V1 : \{\{\{KuG, K12\}K'v2\}, Tc, N2, K12\}K_{v1}$$

The information received by Vehicle 1 by the gateway is to be forwarded to Vehicle 2. This shall assure that the key is shared by its gateway. After performing validation on timestamp vehicle 1 (if the timestamp is validated) gets the shared key. Now, vehicle 1 forwards the public key of Gateway and shared key encrypted with the private key of Vehicle 2 with third nonce value N_3 to vehicle 2. It also sends the current timestamp after concatenation and encryption. Fig. 11 shows the validation process.

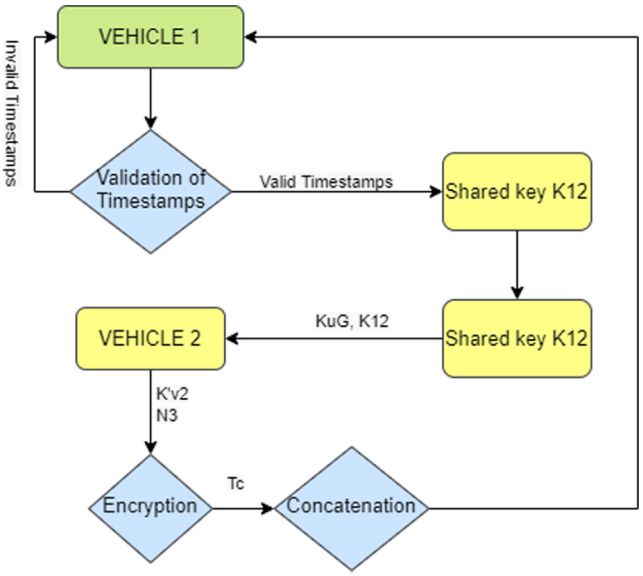


Fig. 11. Validation Process.

$$V1 \rightarrow V2 : \{\{KuG, K12\}bK'v2, \{N3\}K12, H1(K12, Tc)\}K_{v2}$$

Vehicle 2 decrypts the message that it has received and gets a shared key from the public key of the gateway and shared key concatenation with the private key of vehicle 2. This assures vehicle 2 that it has been provided by the gateway. After performing decryption, vehicle 2 gets a third nonce value using the shared key. As vehicle 2 know the hash function and shared key it can now get and perform validation on timestamp. Now, vehicle 2 responds to vehicle 1 with the fourth nonce value $\boldsymbol{N_4}$ after concatenating it with received $\boldsymbol{N_3}$ and valid timestamp. This shall be encrypted by a shared key. This authenticates Vehicle 2 to Vehicle 1. Lastly, vehicle 1 responds with a fourth nonce value encrypted by a shared key which is only known by Vehicle 1 and Vehicle 2, this shall authenticate Vehicle 1 to Vehicle 2.

3.4. Design and validation of proposed scheme

This section explains the implementation of the proposed scheme, and the architecture of Automated Validation of Internet Security Protocol and Applications (AVISPA). This section also breaks down the security properties that AVISPA checks. The execution of the proposed protocol is done in High-Level Protocol Specification Language (HLPSL). It is also exhibited the theoretical reenactment of the proposed scheme. The proposed scheme is designed for the aspects provided in AVISPA. This is an online tool used for verification of internet security-sensitive protocols. This tool performs automated validations and is a role-oriented language. In this tool, each agent that is participating plays a different role during protocol execution. Moreover, each role is purely independent of the other role. An expressive formal language is used in a modular approach for the specification of security properties of the protocol. AVISPA has the integration of different backend setups that are used for analysis techniques for invalidation of the protocol by finding an attack on input. Verification methods used are abstraction-based for finite as well as infinite sessions. Dolev Yao model gives attackers full control over the network, that's why AVISPA uses this model for verifying the strength of the designed protocol. It also verifies the security properties of the specific protocol including authentication, non-repudiation, confidentiality, integrity, and anonymity, and data origin key management. AVISPA is a platform-independent and web-based solution for the verification of designed protocols. The threat model used in this tool is Dolev Yao, it is considered to be the most powerful model that simulates attackers over the network and gives the attacker immense powers over the network for testing out the protocol. It is believed that during testing if the protocol is secure against this model then the protocol is considered to be secure against real-world attacks. Dolev Yao threat model has many capabilities over other threat models:

- The secret data is thought to be indissoluble an attacker doesn't exploit fractional messages. The message is viewed as a secret message except if it is undermined completely.
- The regular role of principals or agents can be assigned to the intruder.
- Messages can be forwarded even if an attacker cannot read them.
- Without the key, decryption cannot be performed.
- The attacker can generate new messages and delete existing messages.
- This is an interactive model where the attacker runs to learn information which can later be used in verification of other protocol.

This tool cannot perform cryptanalysis despite having complete control over the network due to the assumption that the cryptographic primitives used are perfect. This tool uses HLPSL which is a formal language based on a modular approach for modeling communication and security protocols. This is an expressive language that is role-based. AVISPA allows the user to interact by submitting a security problem that can occur and the protocol under verification needs to be tested. The specifications are then translated into Intermediate Format at a lower abstraction level. Foregoing in view, these translations are then served as inputs to the AVISPA backend for verification of the communication and security protocol.

For mathematical processing, this tool uses the following four back-ends which are the primary source of provision for falsification of protocol and bounded unbounded verification:

1. **TA4SP:** is based on Tree Automata, it is dependent on Automatic Approximations for the Analysis of Security Protocols (TA4SP). This back-end indicates the vulnerability in the protocol by careful estimations of intruder capabilities.
2. **CL-AtSe:** stands for Constraint-Logic-based Attack Searcher. It is used to find the possible attacks on a given protocol by translating the specifications into a set of constraints.
3. **OFMC:** stands for On-the-fly Model-Checker. It is utilized for specific protocols with requirements of algebraic properties of cryptographic functions. This back-end is utilized for fast detection of attacks and verification.
4. **SATMC:** is an SAT-based Model-Checker. It generates a propositional formula by taking the transitional state from Intermediate Format to indicate a violation of security properties in a given communication and security protocol.

This tool shows the flaw in a given protocol for a specific secrecy property or strength estimation of the protocol against certain security attacks by computing over-approximation value or under approximation value. The engineering of the AVISPA Tool is portrayed in Fig. 12.

4. Results and discussion

This section explains the results and analysis and explained theoretical analysis and simulation results. The tool AVISPA is used for verification of the proposed protocol. In this section, out of four AVISPA back-ends, OFMC and CL-AtSe back-ends are used which are highly accepted back-ends for this specific purpose. After modeling the proposed protocol in HLPSL protocol specification, SPAN is used as a security protocol animator to symbolically execute the HLPSL protocol specification. Attackers or intruders are not assigned any role during the simulation. In this process, message sequence charts can be generated using SPAN as per specifications written in HLPSL. The tool AVISPA automatically verifies if the designed protocol that is being verified and tested using the same tool satisfies the security properties. This tool is different from other protocol testing tools because it not only gives the assurance that protocol is safe or not but additionally if it finds out that the protocol is unsafe it also gives a trace of the attack found. The security properties of Authentication, Secrecy, and integrity are being verified. Authentication is one of the key property which is based upon authentication property. It is a process of validating a vehicle's identity by other vehicles in communication and vice versa. This ensures the origin and reliability of communication and validates that communication is being done with a legitimate and desirable vehicle. In this proposed protocol, mutual vehicle-to-vehicle authentication is established from a shared session key. This shared key is generated by the gateway and this is transmitted

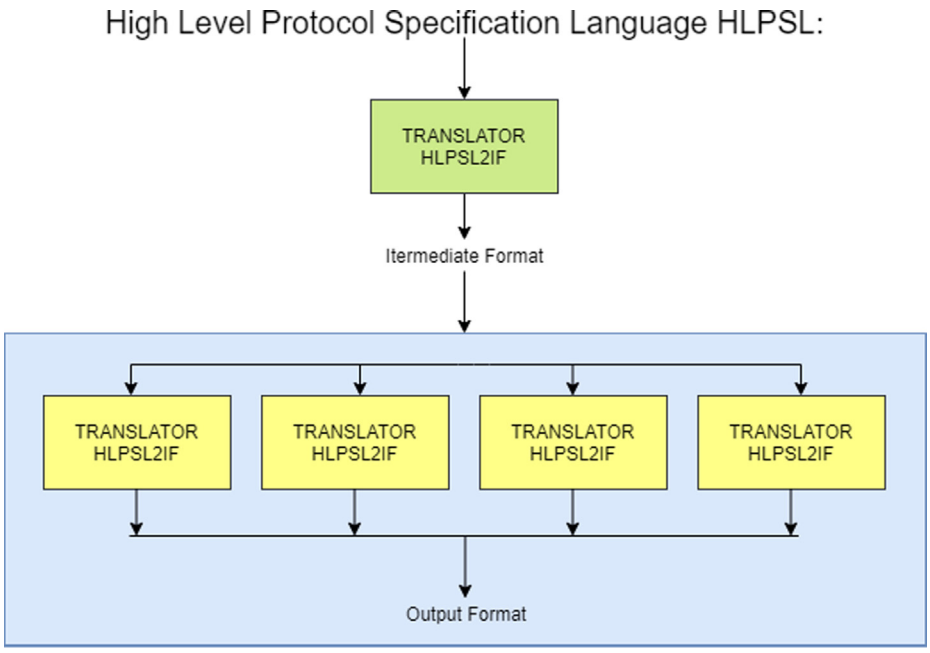


Fig. 12. AVISPA Architecture.

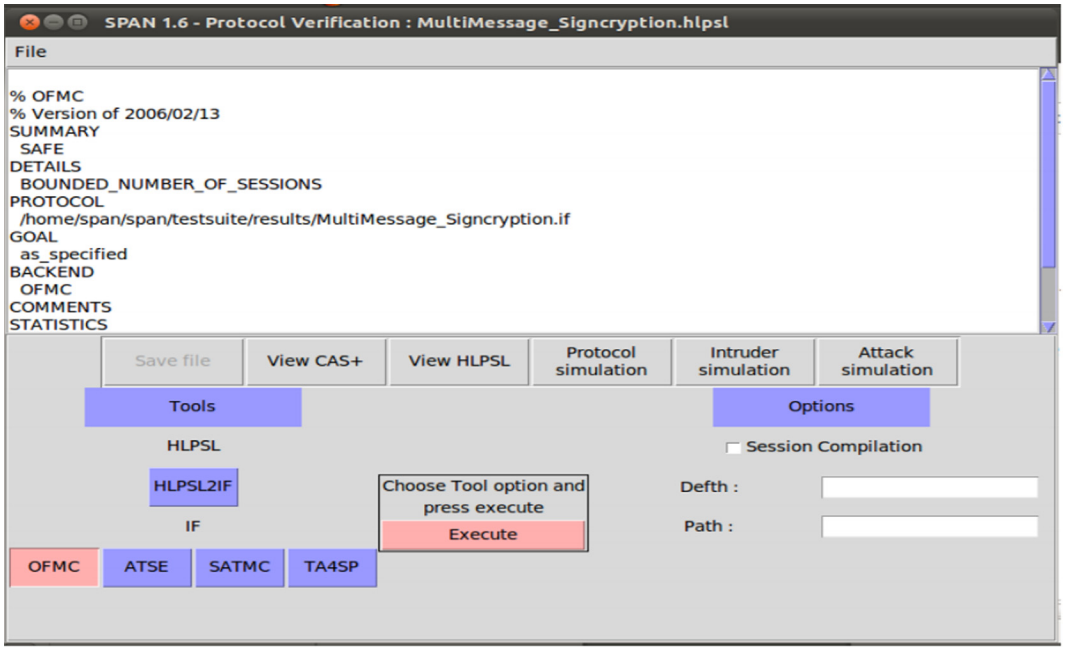


Fig. 13. Protocol verification screenshot.

secretly to only those vehicles who are intended to communicate. Vehicle 1 and vehicle exchange nonce values to authentication themselves to each other. Encryption is done using a private key to ensure the prevention of data breaches.

The property of secrecy ensures the unauthorized access of data/ information for anyone. In other words, the information should only be accessible to those for whom it is intended. This proposed protocol ensures the property of secrecy by keeping all nonce values encrypted and secret during communication. Only intended receivers can decrypt the nonce values and similarly the shared key is also kept secret between communicating parties. The property of integrity implies that the information when received is not been altered or tempered during communication. If this property is maintained, the data received must be in original form from the sender. This proposed protocol is designed keeping in mind the property of integrity by using hash values of the shared session key. Upon receiving, the receiver verifies the hash by using the same algorithm, and in this way, data integrity is ensured.

4.1. Simulation and verification of results

The simulation is performed online using the AVISPA tool after modeling protocol specifications in HLPSL. Afterward, message sequence charts are produced online on a web interface using

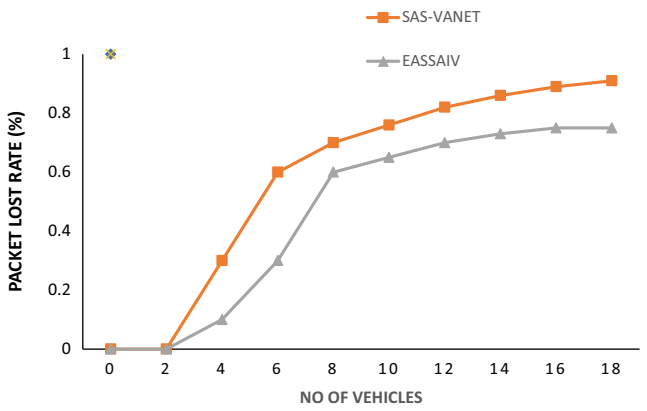


Fig. 14. Packet Loss Rate.

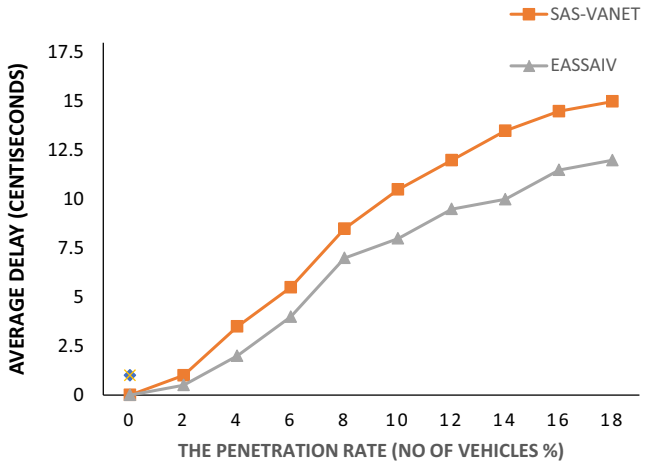


Fig. 15. Average Delay.

SPAN. After this for verifying the model, back-ends are used which are provided in this tool and an active intruder is introduced. OFCM and CL-AtSe back-ends show verification results by confirming the safety of the protocol under both back-ends. This simulation also ensures that the proposed protocol is secure against active or passive attacks. It also indicates that there is no authentication or secrecy attack on the protocol and it is also safe against man in the middle and replays attacks. The shared session key is found safe by having no attack by the intruder. Authentication of participating entities is being done by initiating the exchange of nonce values. Message transmission and secrecy are also found to be intact after the communication. The back-end confirms the absence of any possible attack and found the proposed protocol to be safe. Hash functions are proved to maintain the integrity of communication.

Afterward, the informal security analysis is conducted to evaluate the strength of the proposed protocol against Replay attack, Password Guessing Attack, Multiprotocol Attack, and Reflection Attack. CL-AtSe backend of AVISPA tool is used for detection of Replay and DoS attacks. As discussed above, the proposed protocol is declared safe against these attacks by CL-AtSe. During replay attack, timestamps are used for prevention but additionally use of random nonce values ensure the freshness of the message even if clock synchronization is not in order. Similarly, in Password Guessing Attack, an attacker cannot obtain credentials because of fact the password is not dependent on any credentials. Therefore, the probability of guessing a password is so negligible practically that chance of password guessing compromise is ruled out. Also, various tests are performed to check the performance indexes of the proposed scheme including packet lost rate, average delay, and average data delivery. The results are compared with SAS-VANET [19]. The results of these tests showed promising indicators concerning better efficiency and more productiveness of our proposed scheme in comparison with SAS-VANET. The proposed scheme is validated by using well-known security tool AVISAP. Fig. 13 shows that the proposed scheme is safe and in working condition.

In this regard, the packet loss rate percentage is calculated in comparison with SAS-VANET as shown in Fig. 14. The results showed that the proposed scheme ESSAIV has a steep lower packet lost percentage with a lower number of connected vehicles with a greater difference. With increased vehicles connected at one time showed almost consistent results of EASSAIV with SAS-VANET.

Similarly, during the average packet delay test as shown in Fig. 15, EASSAIV again proved to be a more efficient scheme when compared with SAS-VANET. This test shows the average delay in comparison with the penetration rate among several vehicles in percentage. The results show that throughout the increasing percentage of vehicles (the penetration rate) the average packet delay

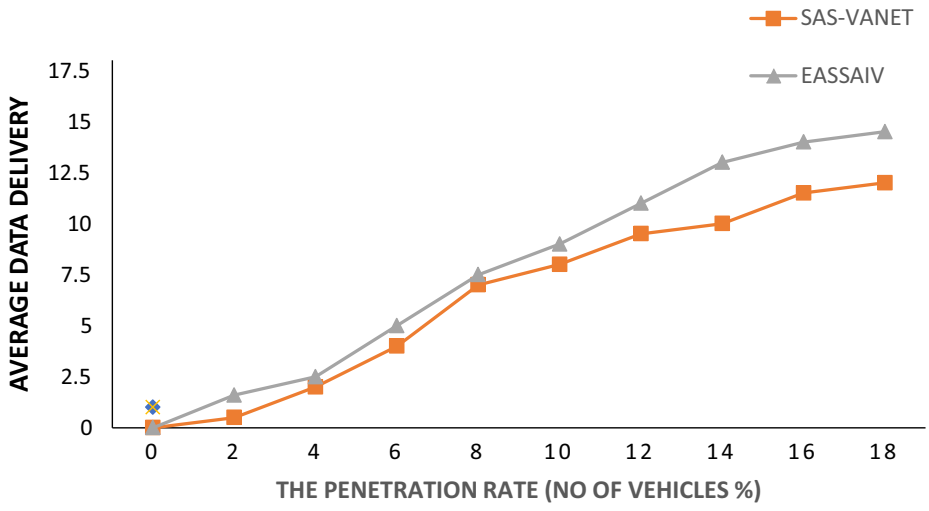


Fig. 16. Average Data Delivery.

of EASSAIV is less than the SAS-VANET scheme. When 18 vehicles are connected using ESSAIV the average delay is 12 cent seconds as compared to 15 cent seconds in SAS-VANET with the same number of connected vehicles.

Subsequently, to further support the proposed scheme, the Average Data Delivery as shown in Fig. 16 test is also performed in comparison with SAS-VANET. The parameters for measuring the said is to compare average data delivery with several connected vehicles. In this test proposed scheme EASSAIV performed better than SAS-VANET by providing a greater data delivery rate with an increased number of connected vehicles in comparison with SAS-VANET. The results show that with 18 vehicles connected, EASSAIV average data delivery rate is 14.5 in comparison with 12 of SAS-VANET with the same number of vehicles.

These results show the efficiency of the proposed scheme over an existing scheme and thus this protocol to be practically usable in real-world scenarios with great potential of expansion possibilities in the future in terms of more efficiency and harnessing of even better results.

5. Conclusion

In this paper, a scheme is introduced for UAV and IoV networks and provide more secure data communication by using authentication mechanism. The proposed EASSAIV is using a mutual message authentication mechanism between drones and vehicles nodes to ensure the security in IoV networks. Most of the existing message authentication schemes do not work on the mutual authentication between nodes. The proposed scheme ensured mutual authentication between vehicle-to-vehicle. The proposed scheme is verified using the AVISPA tool and modeled in SPAN using HLPSL for more practical demonstrations and theoretical evaluations of the results. Simulation results showed the better performance of the proposed scheme compared to the state of the art scheme. This work is also extendible in the future especially for highway environments where the distance between vehicles is another challenge for an authentication mechanism.

Acknowledgment

This work is partly supported with the financial support of the Science Foundation Ireland grant 13/RC/2094_P2 and partly funded from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 754489.

References

[1] Qureshi KN, Din S, Jeon G, Piccialli F. Internet of vehicles: key technologies, network model, solutions and challenges with future aspects. IEEE Trans Intell Transp Syst 2021;22(3):1777–86.
[2] Qureshi KN, Idrees MM, Lloret J, Bosch I. Self-assessment based clustering data dissemination for sparse and dense traffic conditions for internet of vehicles. IEEE Access 2020;8:10363–72.
[3] Duan W, Gu J, Wen M, Zhang G, Ji Y, Mumtaz S. Emerging technologies for 5G-IoV networks: applications, trends and opportunities. IEEE Network 2020;34(5):283–9.
[4] Qureshi KN, Din S, Jeon G, Piccialli F. Link quality and energy utilization based preferable next hop selection routing for wireless body area networks. Comput Commun 2020;149:382–92.
[5] Qureshi KN, Abdullah AH, Lloret J, Altameem A. Road-aware routing strategies for vehicular ad hoc networks: characteristics and comparisons. Int J Distrib Sens Netw 2016;12(3):1605734.
[6] Angurala M, Bala M, Bamber SS. Wireless battery recharging through UAV in wireless sensor networks. Egyptian Inf J 2021.
[7] Islam S. Security property validation of the sensor network encryption protocol (snep). Computers 2015;4(3):215–33.
[8] Alwateer M, Loke SW, Fernando N. Enabling drone services: drone crowdsourcing and drone scripting. IEEE Access 2019;7:110035–49.
[9] Qureshi KN, Abdullah AH, Yusof R. Position-based routing protocols of vehicular Ad hoc networks & applicability in typical road situation. Life Sci J 2013;10(4):905–13.
[10] Qureshi KN, Abdullah H. Topology based routing protocols for vanet and their comparison with manet. J Theoretical Appl Inf Technol 2013;58(3):707–15.
[11] Qureshi KN, Bashir F, Abdullah AH. Distance and signal quality aware next hop selection routing protocol for vehicular ad hoc networks. Neural Comput Applications 2020;32(7):2351–64.
[12] Sakiz F, Sen S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Netw 2017;61:33–50.
[13] Kang J, Xiong Z, Niyato D, Ye D, Kim DI, Zhao J. Toward secure blockchain-enabled Internet of Vehicles: optimizing consensus management using reputation and contract theory. IEEE Trans Veh Technol 2019;68(3):2906–20.
[14] Qureshi KN, Iftikhar A, Bhatti SN, Piccialli F, Giampaolo F, Jeon G. Trust management and evaluation for edge intelligence in the internet of things. Eng Appl Artif Intell 2020;94:103756.
[15] Sun G, Sun S, Sun J, Yu H, Du X, Guizani M. Security and privacy preservation in fog-based crowd sensing on the internet of vehicles. J Network Comp Appl 2019;134:89–99.
[16] Chen C-M, Xiang B, Liu Y, Wang K-H. A secure authentication protocol for internet of vehicles. IEEE Access 2019;7:12047–57.
[17] Li F, Zhang H, Gao L, Wang J, Sanin C, Szczerbicki E. A set of experience-based smart synergy security mechanism in internet of vehicles. Cybernet Syst 2019;50(2):230–7.
[18] Wazid M, Bagga P, Das AK, Shetty S, Rodrigues JJ, Park YH. AKM-IoV: authenticated key management protocol in fog computing-based Internet of vehicles deployment. IEEE Internet Things J 2019;6(5):8804–17.
[19] Bayat M, Barmshoory M, Rahimi M, Aref MR. A secure authentication scheme for VANETs with batch verification. Wireless Netw 2015;21(5):1733–43.
[20] Zhou Y, Liu S, Xiao M, Deng S, Wang X. An efficient V2I authentication scheme for VANETs. Mobile Inf Syst 2018;2018:1–11.
[21] Kong Q, Lu R, Ma M, Bao H. A privacy-preserving sensory data sharing scheme in Internet of Vehicles. Future Generat Comp Syst 2019;92:644–55.
[22] Onieva JA, Rios R, Roman R, Lopez J. Edge-assisted vehicular networks security. IEEE Internet Things J 2019;6(5):8038–45.
[23] Li K, Lau WF, Au MH, Ho I-W-H, Wang Y. Efficient Message authentication with revocation transparency using blockchain for vehicular networks. Comput Electr Eng 2020;86:106721.
[24] Manivannan D, Moni SS, Zeadally S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). Vehicular Commun 2020:100247.
[25] Amin R, Lohani P, Ekka M, Chourasia S, Vollala S. An enhanced anonymity resilience security protocol for vehicular ad-hoc network with Scyther simulation. Comput Electr Eng 2020;82:106554.
[26] Qureshi KN, Bashir F, Abdullah AH. Provision of security in vehicular Ad hoc networks through an intelligent secure routing scheme. In: 2017 International Conference on Frontiers of Information Technology (FIT). IEEE; 2017. p. 200–5.
[27] Alouache L, Nguyen N, Aliouat M, Chelouah R. Survey on IoV routing protocols: security and network architecture. Int J Commun Syst 2019;32(2):e3849.