Computer & Robotics

SMAK-IOV: Secure Mutual Authentication Scheme and Key Exchange Protocol in Fog Based IoV

Yashar Salami [a], Vahid Khajehvand [a, *]

[a] *Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran*

Received 22 November 2020; Accepted 19 April 2021

Abstract

Internet of Vehicles (IOV) is a section of the Internet of Things (IoT) which makes road transportation smart and provides security for the passengers traveling along the roads. Fog computation can be considered as a complement for IOV because it is close to the user and can communicate with Road Side Units (RSU) and process information with low latency. IOV employs a wireless network for message exchange which is a security flaw and an opportunity for the adversaries since that can modify the transmitted data. Thus, data authentication between the transmitter and the receiver has become a challenge in this context. We propose a secure mutual authentication protocol with the ability to key exchange in this paper, which does not use the hash function. We compared this design with other protocols in terms of security requirements and communication and processing costs. To the security analysis of the proposed Automated Validation of Internet Security Protocols and Applications (AVISPA) tool is used. The results show that the proposed protocol is more resistant to other methods of active and passive attacks but Computation and communication costs have increased.

Keywords: (Authentication, Security, Model-Checker, OFMC, CL-ATSE, Avispa)

1. Introduction

In the recent decade, cloud computing has attracted attention as a novel and advanced pattern in information technology, because the purpose of cloud computing is to provide the required sources for the users without considering their location [1]. Scalability and reducing operational costs and easy access to sources are the reasons that cloud computing has attracted attention [2].

Along with cloud computing, traveling has also developed significantly and established a connection between physical objects and digital world [3]. IoT has made a great evolution in daily life by connecting things and human and it has shown proper performance in smart homes, healthcare, and data transmission [4]. As shown in Figure 1, IOT can be divided into 4 fields (M2M, IOV, IOS, and IOE).

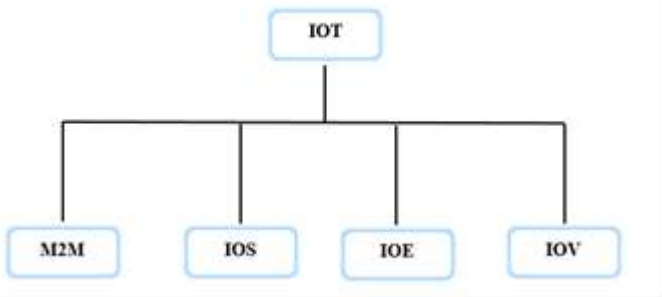

Fig.1 Environments in the IoT.

* Corresponding author. Email:Vahidkhajehvand@gmail.com

In Machines to Machines (M2M) communication, machines communicate with their surrounding machines via their internal network without human interference[5]. Internet of Energy (IOE) is mainly focused on energy [6] and the Internet of Sensor (IOS) is focused on sensors that sense data from the environment [7].

IoV is comprised of Vanet and IoT which has an On-board Unit (OBU) that can store, process, and communicate [8][3]. IoV is an integrated network that manages smart traffic and smart vehicle monitoring and it can be used to handle various traffic and driving problems to provide a secure and easy trip [9]. Fog computation is an applied technology for IoV which is close to the user and can process data and introduce auxiliary latency to the network [10]. Machine and Fog are connected via RSU [8].

Group-based authentication in V2V communications by Hasrouny and Bassil in 2015, [11] But it does not support key exchange and has a high computational cost. In 2017, Yang and Wang dual authentication scheme with security and privacy [12] but high communication costs and does not support fog computing. Ensuring Privacy and Authentication for V2V Resource Sharing by Benarous and Kadri in 2017 [13], But does not support key exchange. In 2017, the smart authentication scheme for vehicles proposed by Mohit and Amin [14] However, this scheme not secure. Anonymous and Lightweight Authentication for Secure Vehicular by Ying and Nayak in 2017 [15], this protocol weak against Rainbow. Anonymous authentication for IOV was proposed by Liu and Qingqing In 2018 [16] but did not have formal security verification using the AVISPA tool. Lim and Tuladhar in 2019 propose Lidar based V2V authentication system without the involvement of trusted authority and infrastructures [17] but Difficult to detect shadowed vehicular and does not support key exchange. Ming Chen and Xiang Secure Authentication Protocol for Vehicular Network propose in 2019[18], this Protocol does not support fog and key exchange. In 2020, Vasudev and Deshpande Lightweight mutual authentication for Communication in IOV [19] However, it is weak against a Rainbow.

Different authentication schemes based on ECC have been proposed in the previous [20]. Kalra and Sood have proposed an authentication method between IoT and cloud [21]. However, it suffers from an Insider attack, Offline password guessing attack. Kumari and Karuppiah have proposed a secure authentication method between IoT and cloud in 2017 using ECC cryptography [22] this method cannot exchange keys. Wazid and Bagga proposed an authentication method using key management for IoV in 2019 [23]. However, this method suffers from the Rainbow table attack. Therefore, privacy and security problems like man-in-the-middle, replay, and session key leakage are important in IoV communication media. To prevent these attacks, the network should be equipped with a secure mutual authentication method that can cover all these issues. Table 1 compares related work and also shows the importance of secure mutual authentication.

Table 1
Comparison of related work.

Related work	Fog Base	Rainbow table	Mutual Authentication	Key Exchange
Hasrouny and Bassil [11]	*x*	*x*	*x*	*x*
Yang and Wang [12]	*x*	*x*	*x*	✓
Benarous and Kadri [13]	*x*	*x*	✓	*x*
Mohit and Amin [14]	✓	*x*	✓	*x*
Ying and Nayak [15]	*x*	*x*	*x*	✓
Liu and Qingqing [16]	*x*	*x*	✓	*x*
Lim and Tuladhar [17]	*x*	*x*	*x*	*x*
Ming Chen and Xiang [18]	*x*	*x*	*x*	*x*
Vasudev and Deshpande [19]	*x*	*x*	✓	*x*
Kalra and Sood [21]	✓	*x*	✓	*x*
Kumari and Karuppiah [22]	✓	*x*	✓	*x*
Wazid and Bagga [23]	✓	*x*	✓	*x*
Proposed scheme	✓	✓	✓	✓

✓: The scheme is supported. X: The scheme is not supported.

1.1. Paper Contribution

The schemes provided for authentication in the IOV environment uses the hash function. The hash function can be decoded using the Rainbow attack, which is ignored in most of the presented works. Without using the hash function, we present a secure authentication protocol based on public key for IoV based on Fog computation. Our protocol with a Mutual authentication establishes key exchange based on the Diffie-Hellman method for IOV devices. Moreover, formal security verification of the proposed scheme using the popular "Automated Validation of Internet Security Protocols and Applications (AVISPA)"

tool proves that the proposed protocol is robust against active and passive attacks.

1.2 Paper Organization

The rest of the paper is organized as follows: In section 2, information about Diffie–Hellman Key Exchange and Network Model. The proposed scheme has been presented in section 3. Section 4 Security Analysis of the proposed Scheme. The comparison and Computation and communications cast and Security requirements in section5. Finally, conclusions have been presented in Section 6.

2. The Background

This section provides a brief introduction to the Diffie–Hellman Key Exchange and Network Model.

2.1. Diffie–Hellman Key Exchange

This protocol has been designed by Whitfield Diffie and Martin Hellman Ralph Merkle in 1976 and was published as a scientific paper. Using the Diffie-Hellman key exchange protocol, two people or two organizations can generate a shared key, not requiring any previous acquaintance, and the can exchange it through an insecure communication path. This protocol is the first practical method for exchanging the key in the insecure communication paths which solves the problem of key exchange in the encryption of symmetric keys[24], [25]**.** Figure 2 shows the Diffie-Hellman key exchange.

2.2. Network Model

Figure 3 shows a model of IoV network connections which shows the connection of the parties. There are various communication states in this model including Vehicles to Vehicles (V2V), Vehicles to RSU (V2R), and RSU to Fog (R2F), Fog to Fog (F2F) and Fog to Cloud (F2C). After loading the information in its memory, RSU transmits a version of the information to the Fog servers and a backup version is stored in the cloud. Rsu can store information in itself. But if there was no information available, they could get the information they needed from Fog It causes lower latency is imposed on the network. In this work, we provide the details of the authentication process for the following cases: 1) Car to RSU, 2) RSU to Fog server, 3) Fog server to cloud server. 4) Car to Car. After a successful authentication process, finally, the key exchange is done. It is also assumed that all vehicles and fog server are they have the same time clock.

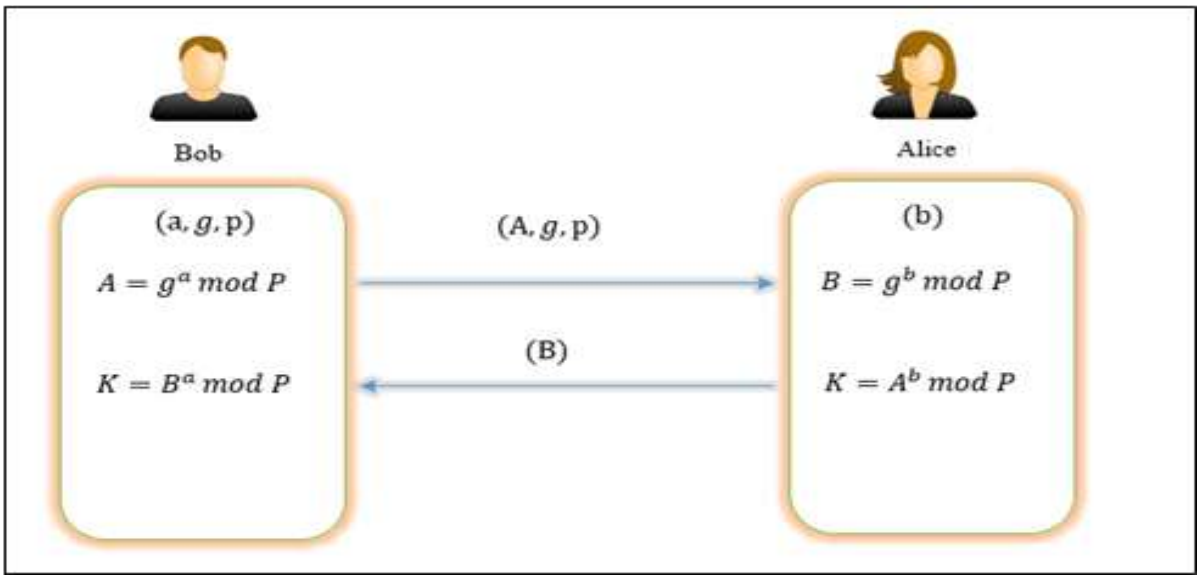

Fig. 2. Diffie–Hellman Key Exchange Phase.

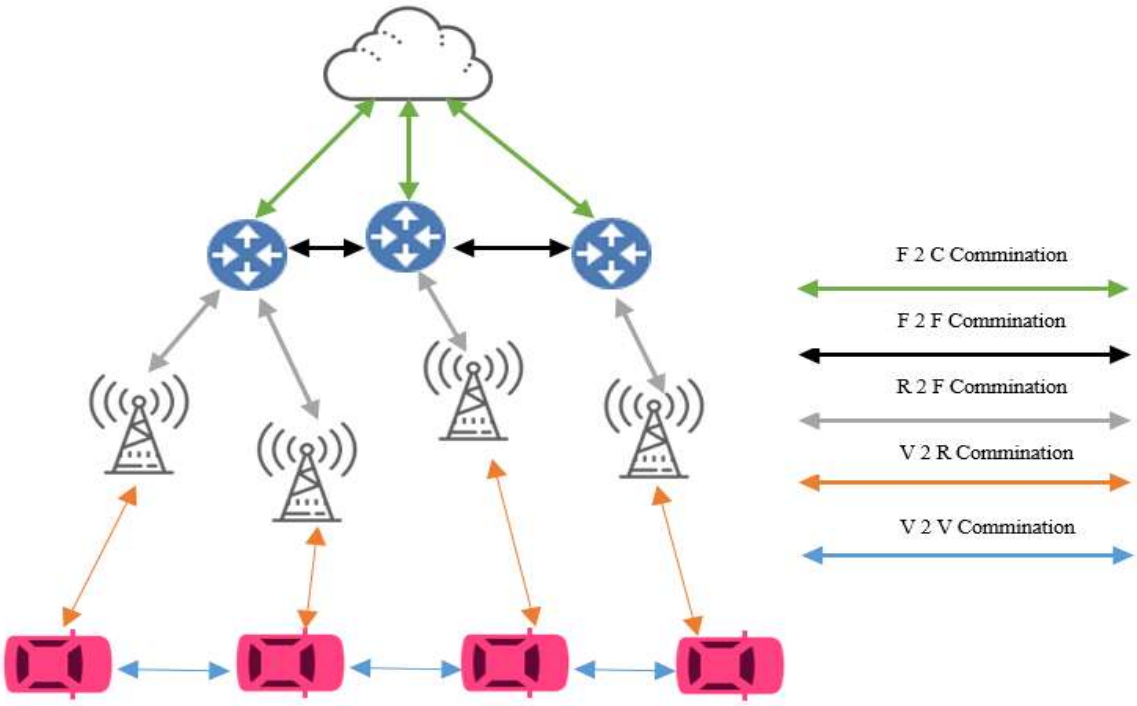

Fig. 3. The network environment of fog computing and IOV.

3. The Proposed Scheme

In this section, we describe various phases related to our proposed scheme. The proposed phase of the authentication the following: In the first phase Initialization and Registration, in the second phase Login and authentication, and finally, the key exchange takes place.

3.1. Notations

Using diagrams or descriptions which are presented in natural language is very useful and transfers the data to the reader very fast. But, for formal and accurate description such that no natural language is required, using diagram alone will not suffice particularly when it is required to prove comprehensiveness and inconsistency in a mechanism or security protocol based of formal methods or model checking or decision methods, pseudo-mathematical symbols should be used for describing authentication mechanisms or other security systems. The list of Notations used in this paper is represented in Table 2.

Table 2
Notations utilized for propose.

No.	Notations	Description
1	A	ntity of Car A
2	B	ntity of Car B
3	F	ntity of Fog
4	M	mmon ID
5	N_A	llenging of Car A
6	N_B	llenging of Car B
7	T	nestamp
8	K_{AS}	public key of Car A
9	K_{BS}	public key of Car B
10	K_{FS}	public key of Fog
11	K_{AB}	mmetric key of Car B and Car A
12	K_{Aex}	mbers for Key Exchange (G,P,A)
13	K_{Bex}	mbers for Key Exchange (B)

3.2. Initialization and registration phase

In the first step, each vehicle selects one of the public key algorithms which has proper security and generates one public key and one private key and then transmits the generated public key to RSU. RSU checks the transmitted public key to see if it is

registered or not. If it is the first time, RSU transmits the public key to Fog and cloud as a backup version so that the vehicle of interest does not need to connect to the network. RSU also selects one of the public key algorithms and transmits the generated public key along with an expiry time for the transmitted packet for each vehicle. It is assumed that the transmission is performed via a secure channel.

3.3. Login and authentication phase

Step LA1:

$$A \rightarrow F : M, A, F, \{N_A, M, A, F, B, T\}_{K_{FS}}$$

A trnsamits a message to F containing identities of A, M, and F and encrypts a challenge for F along with the public key request of B and T for an expiry time of the packet along with identities of A, M, and F with the public key KFS.

Step LA2:

$$F \rightarrow A : M, F, A, \{N_A, M, A, F, B, T, Kbs, Kab\}_{K_{AS}}$$

Upon receiving the message transmitted by A, F decrypts the packet with its private key and checks expiry time of the packet, if it is ended, it requests the message to be transmitted again; otherwise, it generates a message with the previous characteristics and generates the public key of B and the shared key Kab and transmits them with NA and T to A.

Step LA3:

$$A \rightarrow B : M, A, B, \{N_A, M, A, B, T, Kas\}_{K_{BS}}$$

A decrypts the message transmitted by F using its private key and obtains the public key of B and the shared key Kab. A encrypts a message with identities of M, A, and B and transmits a message to B containing NA, M, A, B, T, Kas with the public key B.

Step LA4:

$$B \rightarrow F : M, B, F, \{N_B, M, B, F, A, T\}_{K_{FS}}$$

B decrypts the message received from A with its private key and checks the expiry time of the packet. If the packet is valid, B encrypts a message with identities M, B, and F followed by M, B, F, A, and T with NB which is a challenge from B with the public key of F.

Step LA5:

$$F \rightarrow B : M, F, B, \{N_B, M, B, F, A, T, Kbs, Kab\}_{K_{BS}}$$

Upon receiving message B, F decrypts the message with its private key and checks expiry time of the packet; if it is not valid, it requests the message to be transmitted again; otherwise, it generates a message with the previous characteristics and transmits the public key of A and the shared key Kab along with the response of NB and T to B.

Step LA6:

$$B \rightarrow A :: M, B, A, \{N_A, N_B, M, A, B, T\}_{K_{AS}}$$

B transmits a message with identities A, B, and M and a message encrypt with public key A containing the response to NA and a new challenge NB.

Step LA7:

$$A \rightarrow B : M, A, B, \{N_B, M, A, B, T, \}_{K_{BS}}$$

Upon receiving the message from B, A decrypts the message and responds to the challenge of B via a message. B also ensures to receive the response of its challenge from A.

2.5. Exchange key

Step EK1:

$$A \rightarrow B : M, A, B, \{N_A, M, A, B, T, \mathrm{K_{Aex}}\}_{K_{BS}}$$

A encrypts a message with public key B containing NA, M, A, B, T, KAex. KAex includes three values of A, P, and G generated based on the Diffie-Hellman key exchange.

Step EK2:

$$B \rightarrow A : M, B, A, \{N_A, M, A, B, T, \mathrm{K_{Bex}}\}_{K_{AS}}$$

B decrypts the message transmitted by A and inserts a private key on A, P, and G. KBex is encoded by public key A and transmitted to A; thus, both parties have exchanged a key. The login and authentication and Exchange key phases are given in Figure4.

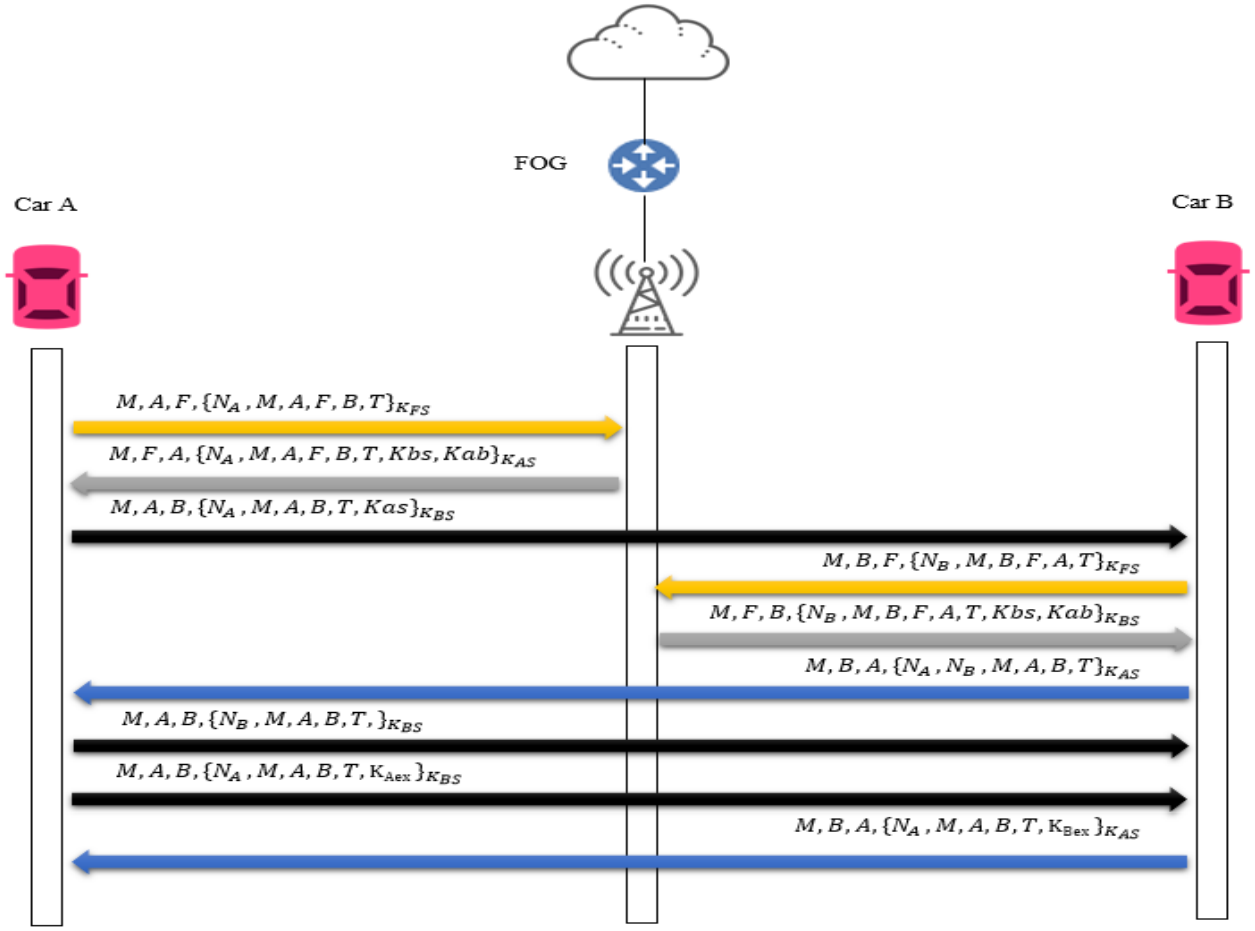

Fig .4. Login and authentication phase.

4. Security Analysis

In this section, the proposed scheme is analyzed and results are presented using AVISPA.

The formal methods used to validate the correctness of the security protocol. The Avispa is performed as a formal verification tool to prove the protocol security. AVISPA is a modular and expressive formal language for specifying protocols and their security features [26]. AVISPA includes of four parts: First Part one On-the-fly Model-Checker (OFMC), Second Part Constraint Logic-based Attack Searcher (CL-ATSE), third part SAT-based Model-Checker (SATMC) and fourth part Tree Automata

based on Automatic Approximations for the Analysis of Security Protocols (TA4SP) [27], [28]. A detailed explanation of these is available in and. The security protocols require to be implemented in the HLPSL (High-Level Protocols Specification Language) [29]. To formally analyze the authentication protocol using the AVISPA tool, the following steps are executed.

- **Step 1**: The protocol is represented in the CAS+ specification.
- **Step 2**: convert CAS+ code to HLPSL
- **Step 3**: Using the translator HLPSL2IF, the HLPSL code is to be converted into IF.
- **Step 4**: The translated IF specification is input to the AVISPA.

As can be seen in Figures 5 and 6 implemented using OFMC and ATSE and the results show the security of the proposed protocol. The simulation output results show that this protocol is safe.

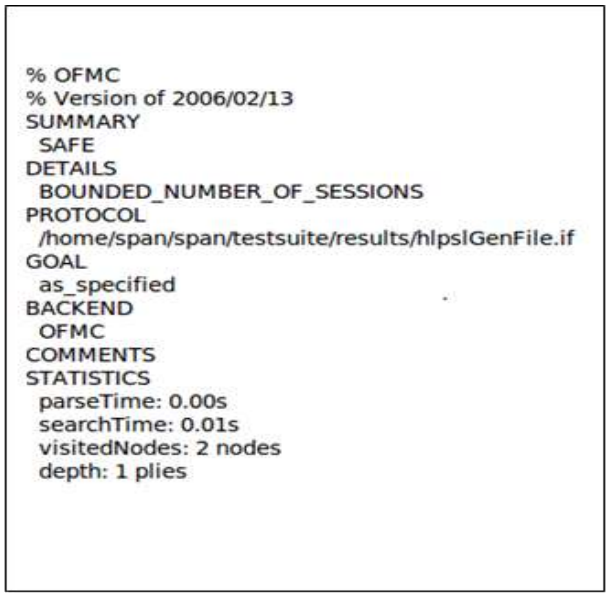

Fig. 5. Result SMAK-IOV on the OFMC Model Checker.

5. Performance Analysis

In this section, we compare the security requirements and performance of the proposed Scheme. The following notations are defined for performance analysis*:*

- Th is the execution number of a hash operation.
- Tecm is the execution number of an ECC point multiplication operation.
- Pe is the execution number of public key encryption.
- Pd is the execution number of public key decryption.
- Se is the execution number of symmetric key encryption.
- Sd is the execution number of symmetric key decryption.

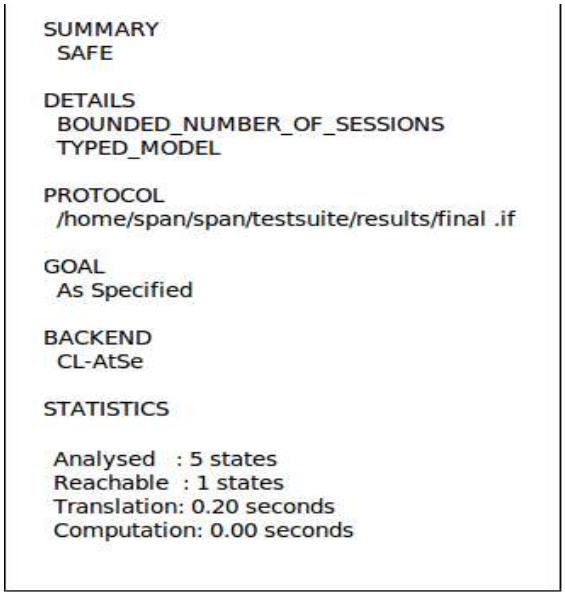

Fig. 6. Result SMAK-IOV on the CL-ATSE Attack Searcher.

5.1 Computation cost

Protocol Wazid and Bagga have a high processing cost, followed by Protocol Mohit and Amin at 20, and with a reduction of one unit, Protocols Liu and Wang and the proposed scheme. The cost of protocols Vasudev and Deshpande and Ming Chen and Xiang are 17 and are one unit of reduction of protocols Liu and Qingqing and Kalra and Sood. Finally, Protocols Kumari and Karuppiah and Ying and Nayak are at 15 and 14 at the lowest cost, respectively. Figure 7 shows the computation cost of the protocols.

5.2 Communication cost

Protocol Liu and Qingqing have the lowest communication cost, followed by Cost 3 Protocols Kalra and Sood and Kumari and Karuppiah. Protocols Ming Chen and Xiang and Ying and Nayak have a communication cost of 4, and then Protocols Wazid and Bagga and Liu and Wang and Vasudev and Deshpande have a cost of 6. The communication cost of the proposed scheme is equal to Protocol Mohit and Amin. Figure 8 shows the Computation cost of the protocols.

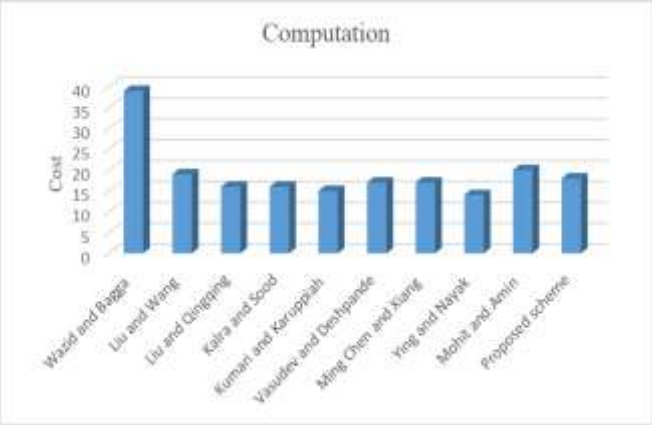

Fig. 7. Comparison of Computation cost.

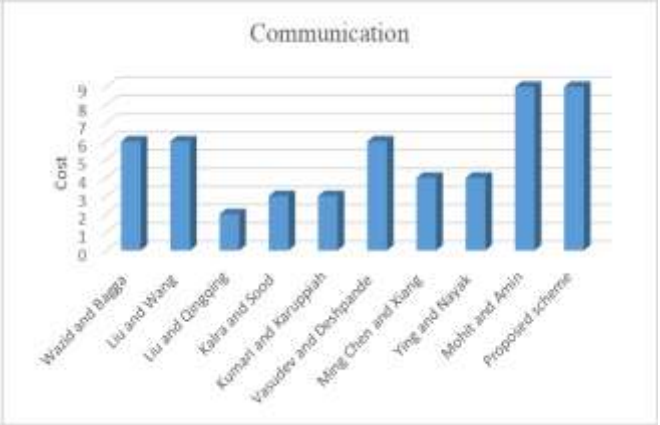

Fig. 8.Comparison of communication cost.

Different schemes are designed based on the hash function. The hash function has a one-way mode, which is why it is so popular, but it is still vulnerable to the Rainbow attack. Today, because the Internet of Things has limited memory and energy, most researchers use elliptical curves. Elliptic curve encryption requires an agreement in the field. In the proposed scheme, we did not use the hash function to counter the Rainbow attack and Elliptical curves require a hash function to send data, which is why we used public-key cryptography. In this scheme, because we did not use the hash function, we had to increase the number of messages exchanged to increase security. Comparison of Computation and communication costs is shown in Table 3.

Table 3
Comparison of communications costs and computation costs.

No.	Schemes	No.of messages	Hash function	ECC	Public key Encryption	Public key Decryption	Symmetric key Encryption	Symmetric key Decryption	Total cost
1	Wazid and Bagga [23]	*6*	*35 Th*	*4Tecm*	*0Pe*	*0Pd*	*0Se*	*0Sd*	*35 Th + 4Tecm*
2	Liu and Wang [12]	*6*	*8 Th*	*11Tecm*	*0Pe*	*0Pd*	*0Se*	*0Sd*	*8 Th + 11Tecm*
3	Liu and Qingqing[16]	*2*	*10 Th*	*6Tecm*	*0Pe*	*0Pd*	*0Se*	*0Sd*	*10 Th + 6Tecm*
4	Kalra and Sood [21]	*3*	*9Th*	*7Tecm*	*0Pe*	*0Pd*	*0Se*	*0Sd*	*9Th + 7Tecm*
5	Kumari and Karuppiah [22]	*3*	*7Th*	*8Tecm*	*0Pe*	*0Pd*	*0Se*	*0Sd*	*7Th + 8Tecm*
6	Vasudev and Deshpande [19]	*6*	*17Th*	*0Tecm*	*0Pe*	*0Pd*	*0Se*	*0Sd*	*17Th*
7	Ming Chen and Xiang [18]	*4*	*17Th*	*0Tecm*	*0Pe*	*0Pd*	*0Se*	*0Sd*	*17Th*
8	Ying and Nayak [15]	*4*	*12Th*	*0Tecm*	*0Pe*	*0Pd*	*2Se*	*2Sd*	*12Th + 2Se +2Sd*
9	Mohit and Amin [14]	*9*	*20Th*	*0Tecm*	*0Pe*	*0Pd*	*0Se*	*0Sd*	*20Th*
10	Proposed scheme	*9*	*0Th*	*0Tecm*	*9Pe*	*9Pd*	*0Se*	*0Sd*	*9Pe+9Pd*

5.3 Security requirements

Table 4 provides a detailed comparison of the proposed method with other available methods. All protocols provided are resistant to replay attacks. Protocol Mohit and Amin against middle man attack and Protocol Kalra and Sood is vulnerable to Insider

attack. Supports most protocols AF4 to AF12 except Protocol Kalra and Sood, which does not support offline password guessing attack, Device anonymity, Mutual authentication, Session key agreement. All protocols are vulnerable to Rainbow attack, the Rainbow attack can break the hash function, so it is a threat to protocols that use the hash function. All protocols are vulnerable to Rainbow attack, the Rainbow attack can break the hash function, so it is a threat to protocols that use the hash function. Our proposed scheme is to protect against the Rainbow attack because we did not use the hash function. Except for our proposed scheme, other protocols do not support key exchange in the fog environment. We checked the security of the proposed scheme from two tools, OFMC and CL-ATSE, Which is less used in the studied protocols. Note: AF1: Replay attack; AF2: Man-in-the-middle attack; AF3: Insider attack; AF4: Stolen-verifier attack; AF5: Impersonation attack; AF6: Brute force attack; AF7: Offline password guessing attack; AF8: Device anonymity; AF9: Mutual authentication; AF10: Session key agreement; AF11: Forward secrecy; AF12: Confidentiality; AF13: Rainbow table, AF14: Key Exchange, AF15: OFMC, AF16: CL-ATSE, AF17: Fog Base. ✓: The scheme is supported. X: The scheme is not supported.

Table 4
Security requirements comparison.

Security requirements	Schemes									Proposed scheme
	Wazid and Bagga [23]	Liu and Wang, [12]	Liu and Qingqing[16]	Kalra and Sood [21]	mari and Karuppiah [22]	idev and Deshpande [19]	ng Chen and Xiang [18]	Ying and Nayak [15]	Mohit and Amin [14]	
AF1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AF2	✓	✓	✓	✓	✓	✓	✓	✓	x	✓
AF3	✓	✓	✓	x	✓	✓	✓	✓	✓	✓
AF4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AF5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AF6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AF7	✓	✓	✓	x	✓	✓	✓	✓	✓	✓
AF8	✓	✓	✓	x	✓	✓	✓	✓	✓	✓
AF9	✓	✓	✓	x	✓	✓	✓	✓	✓	✓
AF10	✓	✓	✓	x	✓	✓	✓	✓	✓	✓
AF11	✓	✓	✓	x	✓	✓	✓	✓	✓	✓
AF12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AF13	x	x	x	x	x	x	x	x	x	✓
AF14	x	x	x	x	x	x	x	✓	x	✓
AF15	✓	x	x	✓	✓	x	x	x	x	✓
AF16	✓	x	x	✓	x	x	x	x	x	✓
AF17	✓	x	x	x	x	x	x	x	x	✓

5. Conclusion

People inside vehicles or around vehicles communicate with the urban environment via IOV which is due to the fast development of Fog. The security of IOV is one of the main challenges in this context. A secure authentication protocol with the ability to exchange key is presented in this study which can provide mutual authentication for both parties. Previous designs were not resistant to the Rainbow attack and could not provide security necessities for authentication. To evaluate the proposed protocol, Avispa is used which shows that the proposed protocol is robust against active and passive attacks and it is well designed for IoV. In the future, we are going to reduce the communication and computation cost of the proposed protocol.

References

[1] T. Mastelic, A. Oleksiak, H. Claussen, I. Brandic, J.-M. Pierson, and A. V Vasilakos, "Cloud Computing: Survey on Energy Efficiency," *ACM Comput. Surv.*, vol. 47, no. 2, Dec. 2014.

[2] M. Xu and R. Buyya, "Brownout approach for adaptive management of resources and applications in cloud computing systems: A taxonomy and future directions," *ACM Comput. Surv.*, vol. 52, no. 1, 2019.

[3] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Veh. Commun.*, vol. 20, pp. 100–182, 2019.

[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[5] S. Andreev *et al.*, "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 32–40, 2015.

[6] M. H. Yaghmaee Moghaddam and A. Leon-Garcia, "A fog-based internet of energy architecture for transactive energy management systems," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1055–1069, Apr. 2018.

[7] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *Secur. Commun. Networks*, vol. 2017, 2017.

[8] M. Ma, D. He, H. Wang, N. Kumar, and K. K. R. Choo, "An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8065–8075, 2019.

[9] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Informatics*, vol. 14, no. 10, pp. 4568–4578, 2018.

[10] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions," pp. 103–130, 2018.

[11] H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, "Group-based authentication in V2V communications," in *2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 2015, pp. 173–177.

[12] Y. Liu, Y. Wang, and G. Chang, "Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, 2017.

[13] L. Benarous and B. Kadri, "Ensuring privacy and authentication for V2V resource sharing," *Proc. - 2017 7th Int. Conf. Emerg. Secur. Technol. EST 2017*, pp. 1–6, 2017.

[14] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Veh. Commun.*, vol. 9, no. February, pp. 64–71, 2017.

[15] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, 2017.

[16] J. Liu, Q. Li, R. Sun, X. Du, and M. Guizani, "An efficient anonymous authentication scheme for internet of vehicles," *IEEE Int. Conf. Commun.*, vol. 2018-May, pp. 1–6, 2018.

[17] K. Lim and K. M. Tuladhar, "LIDAR: Lidar Information based Dynamic V2V Authentication for Roadside Infrastructure-less Vehicular Networks," *2019 16th IEEE Annu. Consum. Commun. Netw. Conf. CCNC 2019*, pp. 1–6, 2019.

[18] C. M. Chen, B. Xiang, Y. Liu, and K. H. Wang, "A secure authentication protocol for internet of vehicles," *IEEE Access*, vol. 7, no. c, pp. 12047–12057, 2019.

[19] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A lightweight mutual authentication protocol for V2V communication in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6709–6717, 2020.

[20] S.-T. Wu, J.-H. Chiu, and B.-C. Chieu, "ID-based remote authentication with smart cards on open distributed system from elliptic curve cryptography," in *2005 IEEE International Conference on Electro Information Technology*, 2005, pp. 5----pp.

[21] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive Mob. Comput.*, vol. 24, pp. 210–223, 2015.

[22] S. Kumari, M. Karuppiah, A. Kumar, D. Xiong, L. Fan, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *J. Supercomput.*, 2017.

[23] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, 2019.

[24] E. Bresson, O. Chevassut, and D. Pointcheval, "Provably secure authenticated group Diffie-Hellman key exchange," *ACM Trans. Inf. Syst. Secur.*, vol. 10, no. 3, pp. 10----es, 2007.

[25] L. Harn, M. Mehta, and W.-J. Hsin, "Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA)," *IEEE Commun. Lett.*, vol. 8, no. 3, pp. 198–200, 2004.

[26] J. A. Hurtado Alegr$\$'$\$ia, M. C. Bastarrica, and A. Bergel, "Analyzing software process models with AVISPA," in *Proceedings of the 2011 International Conference on Software and Systems Process*, 2011, pp. 23–32.

[27] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electron. Notes Theor. Comput. Sci.*, vol. 155, pp. 61–86, 2006.

[28] A. Armando *et al.*, "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications," in *Computer Aided Verification*, 2005, pp. 281–285.

[29] D. Von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proceedings of APPSEM 2005 workshop*, 2005, pp. 1–17.