ASTEEC Conference Proceeding: Computer Science
3rd International Conference on Information Science and Technology Innovation (ICoSTEC)
July 27, 2024, Yogyakarta, Indonesia

Survey of authentication model for Vehicular Ad Hoc Networks

Abdelilah El ihyaoui1 , My Abdelkader Youssefi2, Ahmed Mouhsen3

Hassan First University of Settat , Faculté des Sciences et Technique ,
cHassan First University of Settat , Faculté des Sciences et Technique ,

Laboratoire d'Ingénierie, de Management Industriel et d'Innovation (LIMII), Morocco
[1]abdelilah.elihyawi@gmail.com
[2]ab.youssefi@gmail.com
[3]mouhsen.ahmed@uhp.ac.ma

Abstract— **Intelligent transport systems (ITS) guarantee the functionality of the parts used in vehicular networks and the creation of security models that assure system protection. Our work consists of concentrating particularly on the component authentication techniques. Only the authenticated components can consequently have the privileges to exchange messages because, in the absence of adequate security models, the information shared between system components can serve as sources of risks that directly affect people's lives. Given the importance of the topic in recent years, a number of security models have been put forth to safeguard user life and identity.**

***Keywords*— V2V, security; hash message authentication code (HMAC), access token; authentication, vehicular ad hoc networks (VANETs).**

I. Introduction

Vehicle ad hoc network systems have a network type that is specific to mobile vehicles and a fixed infrastructure with a reliable regional authority and an RSU. By exchanging data, such as the position, speed, and direction of vehicles as well as warnings of impending dangers like accidents and embankments, VANET networks facilitate traffic and enhance road safety [1]. Additionally, it offers comfort services to drivers, but in order to ensure proper operation, vulnerabilities and malicious attacks must be prevented. Several authentication models have been put forth to accomplish this. These models are based on asymmetric cryptography.

Vehicle networks are also subject to the key traditional network design flaws, including DoS (Denial of Service), bogus information, which refers to information transmitted by enemies and includes certifications, security messages, warnings, and fabricated identities [2].

For VANET security, there are a number of crucial elements that are explained below. Authentication: Only messages sent by authorized network users should elicit a response from vehicles. Therefore, verifying the message's sender is necessary [3].

Asymmetric cryptographies are the fundamental tools for securing information, including non-repudiation, data integration, and authentication message privacy [4]. Additionally, traditional networks use CAs (Certificate Authorities) to distribute and manage keys.

There are several systems proposed to ensure the security of messages transmitted across vehicular networks, and the

proposed model can be divided into four types. Group identity-based, blockchain-based, and signature-based technologies.

II. Authentication models

We discuss research that has been published in the literature on the safety of V2V and V2I communications.

There are several systems proposed to ensure the security of messages transmitted across vehicular networks, and the proposed model can be divided into four types. identity-based, Public Key infrastructure-based, blockchain-based, and Groupe signature-based technologies.

In a different strategy, [3] the author prevents using the TPD. The idea is to replace the TPD with a pre-paid card that stores the authentication keys. The user's real information is stored with the provider of the card, and messages are intercepted using the provider's public key. The user is given a pseudonym that is valid for a short time in a specific area.

The authors of [4] suggest an authentication system based on asymetric keys. This model enables the vehicle to generate public/private keys, and the latter uses the Diffie-Hellman algorithm to exchange the keys with the RSU upon entering a zone.

Raya and Hubaux [5] present a model that is based on the distribution of thousands of certificates. Like other models, it assumes that the vehicle is equiped with a device (TPD) that can store multiple certificates with false identities. The vehicle then randomly chooses a certificate to sign a message.

With the pseudonyms Efficace and Robuste [6], as shown in Figure 1, the authors (ERPA) rely on the group's signature; CA has a private group gsk-v key and a public group gpk-ca key. Each vehicle has a group signature on the certificate that is verified using gskv after the pseudonym has been added to the certificate. Pseudonymous authentication requires a public key vehicle that conceals the identity. The recipient validates the message of signature using the gpk-ca. The communications are signed with a private key and attached with an associated certificate. This system guarantees the

message's authenticity, integrity, non-repudiation, and anonymity.

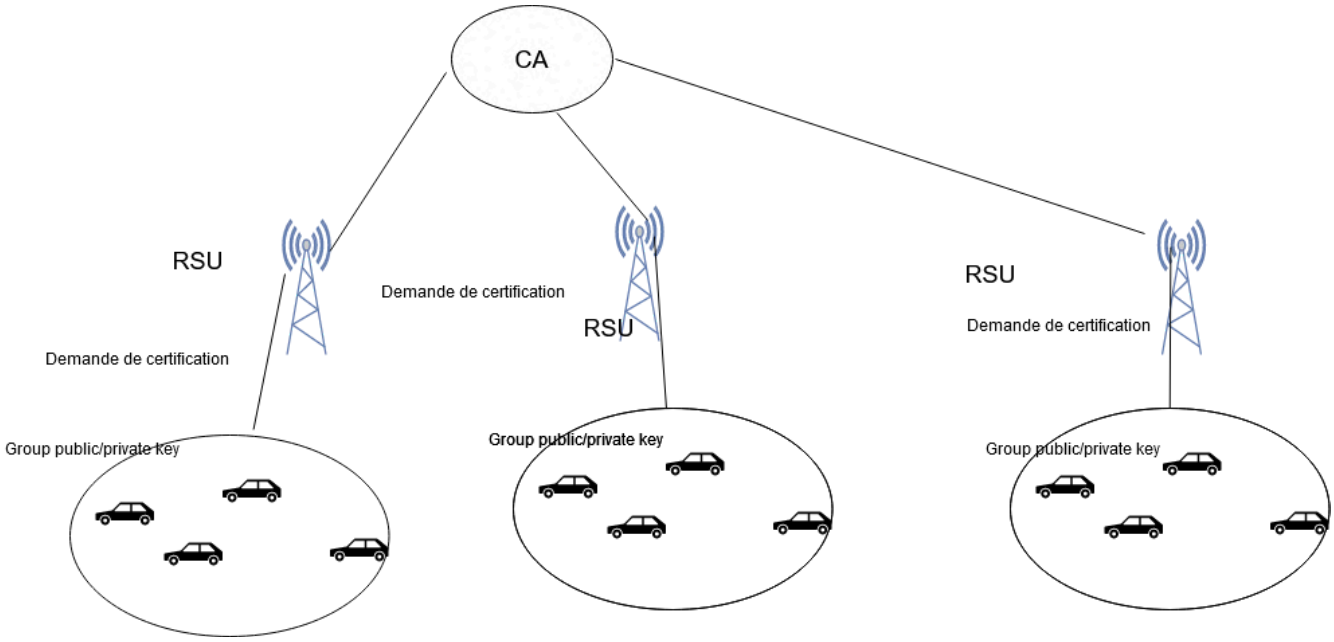

FIG. 1

All title and author details must be in single-column format and must be centered.

TACKs [7] divides the VANET networks into smaller areas, and the CA transfers all responsibilities to the regional authorities (RA). Guk was used by the organization's members to create a group signature. The CRL, which is connected to each regional authority, applies revocation and traceability.

The networks VANET are divided into equilateral segments by the authors of [8], with each segment being run by a separate RSU. The vehicles communicate with the RSU without returning to the CA and share the group clef.

The authentication is described in [9] using a short-lived key that changes frequently; this model makes use of symmetric computation, the RSU, and key distribution. The concept of a transitive relation of confidence, [10] presents a decentralized authentication model for V2V networks to safeguard the vehicles.

Authentification Anonymous Adaptive Probabilistic (PAAA) [12] is focused on anonymity, rapidity, and evolution. The Road Side Unit (RSU) uses public key cryptography to avoid the overload of the CA ; the central server manages the pair of public and private keys, and the subgroup manager distributes the key.

The model [13] proposes a leader for each group in V2V communication; the leader is the vehicle that has been a part of the group for the longest. Asymmetric authentication is used for each node, and identity-based cryptography is used to authenticate the vehicle without the use of certificates. Within the group, the authors assume that mutual vehicle authentication has already been completed with the RSU.

The authors of Anonymous Blockchain Reputation System [14] present a new model that uses two blockchains (CerBc and RevBc) for authentication and uses those blockchains to verify the validity of certificates.

The idea behind public key infrastructure (PKI) [15]authentication schemes is to preload a large anonymous pool of roughly 43,800 certificates along with their private keys at the necessary levels. All certificates are signed by the TA, and they contain no information that might be used to identify the identities of the vehicles, making them completely anonymous. Each vehicle needs to have enough pre-charged certifications to ensure long-term and private security, such as for a year. The certificates could be updated during the vehicle's yearly inspection. Initially, messages related to vehicle traffic are signed by random selection of anonymous certificates and their corresponding private keys. The verification vehicle obtains the signer's public key from the TA, who keeps track of all the certificates issued to vehicles in these schemas, in order to verify a signature using an anonymous certificate. As a result, the TA may ascertain the identities of users as needed.

The biggest issue with a PKI scheme is the revocation process. Since the revocation of many certificates in the certificate list of revocation (CRL) is required by the revocation of the same vehicle, the requirement to charge a large number of vehicle certificates renders the management of a vehicle ineffective. This problem is primarily fatal when the CRL is high. Given that the CRL keeps track of all public keys that have been invoked, the public key must also be authenticated during the signature verification process. On a VANET, however, it is more difficult to confirm the legitimacy of a public key than it is on a standard network.

Simple login and password authentication was the initial authentication method used in conventional networks. Web services currently use a common technique known as knowledge-based authentication, or KBA [19]. The service provider (the authentication server) and the client both need to be familiar with passwords and logins in order to use KBA (the end user device or the owner of the identity). As a result, the effectiveness of authentication depends on the knowledge of a secret that must be disclosed to both the service provider and the user of the end device (the customer). The server of the provider houses this information. By comparing the secret provided by the customer to the secret kept on the server, this method provides authentication.

The model [20] authors present a security model architecture for vehicular communications that offers lightweight, real-time, decentralized, and efficient authentication applicable in real-world scenarios. The proposed model adheres to essential security requirements, including authenticity, anonymity, integrity, and non-repudiation.

The scheme initiates with the authentication between the vehicle and the Road Side Unit (RSU), where the vehicle obtains an Access Token and key to join the group. A Hash Message Authentication Code (HMAC) is employed to avoid time-consuming Certificate Revocation List (CRL) checks. Subsequently, the vehicle uses the generated Access Token for communication. Performance evaluations demonstrate that this model is more efficient in terms of authentication speed and resource consumption.

Traditional security models based on asymmetric cryptography are costly and storage-intensive, making them unsuitable for Vehicular Ad Hoc Networks (VANETs) where Vehicle-to-Vehicle (V2V) communication demands strict real-time processing. Signature verification in these models also adds significant cost and latency.

To meet the real-time requirements of V2V communication, the authors propose a novel three-step authentication strategy:

Initial Registration: Utilizing flexible real-time authentication for Vehicle-to-Infrastructure (V2I) communication.

Access Token Aggregation: Broadcasting aggregated tokens (Haggr) to group vehicles.

Real-Time Authentication: Ensuring secure V2V communication without relying on asymmetric cryptography.

This model ensures efficient and secure real-time authentication, making it well-suited for VANETs and enhancing overall vehicular network security and performance.

III. EVALUTION AND DISCUSSION

In this article, we discussed a variety of authentication models. We noted that the models with strong authentication require large data storage and processing power, which cannot be used in VENET networks due to limited resources and the requirement for real-time communication between all parties. Accordingly, the challenge in VANET networks is to find an effective authentication model.

TABLE I SECURITY MODELS

Security Model	**Communication types**	**Cryptography System**	**Power of authenticity**	**Strength(+) Weakness (-)**
KBA [19]			weak	(+) Computation and storage are low (-) No resistance to DoS attack (-) No real time
[3]	V2V, V2I	Asymmetric	Strong	(-) High storage requirements (-) Increase the computation (-) No real time
[4]	V2V, V2I	Asymmetric	Strong	(-) High storage requirements (-) Increase the computation (-) No real time
[5]	V2V, V2I	Asymmetric	Strong	(-) High storage requirements (-) Increase the computation (-) No real time
Probabilistic adaptive anonymous authentication (PAAA) [12]	V2V, V2I	Asymmetric	Strong	(-) High storage requirements (-) Increase the computation (-) No real time

Efficient and Robust Pseudonymous Authentication (ERPA) [6]	V2V, V2I	Asymmetric	Medium	(+) low storage (-) Increase the computation (-) No real time
TACKs [7]	V2V, V2I	Asymmetric	Medium	(+) low storage (-) Increase the computation (-) No real time
Group-based V2V [13]	V2V	Asymmetric, Symmetric	Medium	(+) low storage (-) Increase the computation (-) No real time
BARS [14]	V2V, V2I	Asymmetric	Strong	(-) High storage requirements (-) Increase the computation (-) No real time
New efficient authentication model for Vehicular Ad Hoc Networks [20]	V2V, V2I	Asymmetric, (V2I) Symmetric, (V2V)	Strong	(+) low storage (-) Increase the computation (+) Real time

III. Conclusions

This document represents an overview of the current state of research in the field of authentication in VANETs, the V2V communication requires hard real-time, as well as signature verification, which adds a high cost and high latency, security models based on cryptography with these drawbacks—they all employ asymmetric cryptography—cannot be used in VANET networks. Soo the New Efficient Authentication Model for Vehicular Ad Hoc Networks ([20]) emerges as the most promising solution for VANETs, combining the strengths of both asymmetric and symmetric cryptography to achieve strong authenticity, low storage requirements, and real-time communication capabilities. This model addresses the critical needs of VANETs, providing a balanced approach that enhances security and performance while mitigating the common weaknesses found in other models.

References

[1] Tomandl, D Herrmann, Karl-Peter Fuchs, H Federrath and F Scheuer “An open source simulator for security and privacy concepts in VANETs” 2014 International Conference on High Performance Computing & Simulation (HPCS)

[2] Hamssa Hasrouny, Carole Bassil, Abel Ellatif Samhat , Anis Laouiti “Group-Based Authentication in V2V communications” 2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP).

[3] Mohammed Saeed Al-kahtani “Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)” 2012 6th International Conference on Signal Processing and Communication Systems.

[4] Cliff. Aslam Baber, Zou “Distributed Certificate Architecture for VANETs’ IEE Military Communications C onference (MILCOM09), Boston, Oct. 18-21, 2009.

[5] Mahmoud Abuelela, Stephan Olariu, Khaled Ibrahim, “A Secure ans Privacy Aware Data Dissemination For The Notification of Traffic Incidents” In proceeding of IEE Vehicular Technology Conference Avril 2009.

[6] FranN Kargl, “Security and Privacy in C2X Communication”, Communications Magazine, IEEE (Volume:49 , Issue: 5),Page(s):158 – 164

[7] Ashwin Rao, Ashish Sangwan, Arzad A. Kherani Anitha Varghese, Bhargav Bellur, Rajeev Shorey , “Secure V2V Communication With Certificate Revocations”,Published in IEEE Mobile NetworNing for Vehicular Environments 2007

[8] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, “RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks,” in Proc. IEEE Int. Conf. Commun., May 2008, pp. 1451–1457.

[9] BAI Qing-hai “Comparative Research on Two Kinds of Certification Systems of the Public Key Infrastructure (PKI) and the Identity Based Encryption (IBE)” 2012 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference.

[10] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy. Efficient and robust pseudonymous authentication in VANET. VANET '07: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, (New York, NY, USA), pp. 19-28, ACM, 2007.

[11] A. Studer, E. Shi, F. Bai, and A. Perrig. “TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs”. 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks.

[12] MayanN Verma, Dijiang Huang, “SeGCom: Secure Group Communication in VANETs”, Communications and NetworNing, 2009. ComNet 2009. IEEE 2009

[13] Lu Song, Qingtong Han, Jianwei Liu, "Investigate Key Management and Authentication Models in VANETs",IEEE International Conference on Electronics, Communications and Control (ICECC), 2011.

[14] Ming-Chin Chuang, Jeng-Farn Lee,”TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc NetworNs”, Systems Journal, IEEE (Volume:8 , Issue: 3), 2013.

[15] [Michael B. Jones, John Bradley, and Nat Sakimura. JSON Web Token (JWT).2015. https://tools.ietf.org/html/rfc7519.

[16] P. Solapurkar, "Building secure healthcare services using OAuth 2.0 and JSON web token in IOT cloud scenario," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, 2016, pp. 99-104.

[17] Kai Zheng and Weihua Jiang, “A Token Authentication Solution for Hadoop Based on Kerberos Pre-Authentication”, in proc “Data Science and Advance Analytics (DSAA)”, Shanghai, 2014, pp. 354 – 360.

[18] O. Ethelbert, F. F. Moghaddam, P. Wieder and R. Yahyapour, "A JSON Token-Based Authentication and Access Management Schema for Cloud SaaS Applications," 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, 2017, pp. 47-53.

[19] Youssefi My Abdelkader, Mouhsen Ahmed “ A new strong user authentication scheme with local certification authority for internet of things based cloud computing services” International Journal of Advanced Technology and Engineering Exploration, Vol 6(58)

[20] Youssefi My Abdelkader, Mouhsen Ahmed “New efficient authentication model for Vehicular Ad Hoc Networks” Journal of Communications ISSN: 1796-2021 (Online); 2374-4367 (Print) 2022 > Volume 17, No. 7, July 2022