Computer Software and Media Applications (2023) Volume 6 Issue 1
doi: 10.24294/csma.v6i1.3061

ORIGINAL RESEARCH ARTICLE

An optimized secure dual authentication for VANETs

Deepalakshmi Kandeepan*, R. Durga*

Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai 600117, India

*** Corresponding author:** Deepalakshmi Kandeepan, deepalashmi22@gmail.com; R. Durga, drrdurgaresearch@gmail.com

ABSTRACT

"Vehicular Ad-hoc Network (VANET)" has emerged as a hotbed of research and development. This technology has been utilized to improve vehicle and road safety by transmitting information about traffic congestion and road conditions during emergencies in order to soothe drivers and passengers. However, such environments are more vulnerable to security risks. Thus, the primary challenge in such an environment is to provide authentication services while maintaining user confidentiality. To that end, a trustworthy authority (TA) is established, which offers services to users as well as authentication of communications transmitted between trusted authorities and VANET nodes. A trusted authority (TA) is established using VANETs to supply clients with a range of online premium services. As a result, preserving the confidentiality and authenticity of messages conducted between the TA and VANET nodes is crucial. Our proposed method minimizes recognition latency by up to 85% when compared to On-site Driver ID, and decreases authentication latency by up to 94%, respectively.

Keywords: VANET; RSU; dual authentication; trusted authority

ARTICLE INFO

Received: 20 October 2023
Accepted: 11 December 2023
Available online: 26 January 2024

1. Introduction

Time is essence; accidents lead to a waste of time; they cause fatalities, but they also cause traffic congestion. Cars should be supplied with traffic information in a secure and timely manner to alleviate these challenges and boost driving comfort[1]. Many individuals nowadays use cabs to get from one area to another. Traffic congestion and road mortality are caused by the rising number of cars in the road transportation system. By providing vehicle drivers with correct information about road conditions and their surroundings in a safe manner, traffic congestion and road mortality can be reduced. To address these crucial driving issues, automobiles are outfitted with communication technologies that allow information to be exchanged between vehicles as well as between vehicles and Road Side Units (RSUs)[2].

Security services such as road condition updates, traffic sign violation warnings, and emergency vehicle notifications are also provided via VANETs. Weather predictions, traffic updates, gas station or restaurant locations, and Internet connectivity are among the features they can give[3]. RSUs are used to connect autos to the TA and are located along the roadside. An On Board Unit (OBU) is installed in each vehicle, which manages all computer and communication functions. Various statistical studies show that many people have died

or been wounded as a result of road accidents, and traffic bottlenecks waste a lot of time and fuel[4].

The Trusted Authority (TA), RSUs, and vehicles are the three main components of a VANET's basic framework. The VANET's real-time, dynamic communication capabilities enable efficient and continuous information transfer as well as appealing application services, potentially improving drivers' driving experiences dramatically. As a result, an efficient authentication system is required to ensure communication security[5]. The primary goal of VANETs is to offer safety and traffic-related information, which is a key feature of ad hoc network systems. VANET allows cars to send warning signals to other vehicles about road accidents, traffic congestion, and street conditions, as well as information about specific locations. This enables users to pick a less congested route and avoid accident-prone areas for a safe and traffic-free trip[6]. In this research, in order to successfully prevent unauthorized cars from entering the VANET, we provide a dual authentication mechanism for ensuring a high level of security on the vehicle side.

2. Related works

Sayana et al.[7] presented a novel dual authentication technique to improve the security of cars connecting with the VANET. To establish dual mode authentication, we used two components: a hash code and each connecting vehicle user's fingerprint. As a consequence this research combines a fingerprint authentication technique into a process which generates hash code to prohibit unauthorized users from accessing any VANET user's secret or private key and engaging in VANET communication.

The proposes of the Vehicle Ad- hoc Network (VANET) for traffic security and efficiency on roads that was spurred by the possible extension of the Mobile Ad-hoc Network (MANET)[8], since if deployed, they may offer drivers with a new environment. In a real-time situation, vehicular communication creates a considerable privacy barrier, which may limit the adoption of VANETs on a wide scale. Researchers have proposed several solutions to these problems. This study delves into a number of privacy-preserving authentication mechanisms used in vehicular communication.

He et al.[9] introduces many signature-based techniques for authentication in VANETs have been proposed, However, few have addressed the issue of signature-based authentication being subjected to denial of service (DoS) attacks. In this sort of DoS attack, attackers send out fake messages with flawed signatures, causing receiving cars to do several unnecessary signature checks, preventing the benign vehicles from confirming messages from other legitimate vehicles. To counteract a denial-of-service attack of this nature, He et al. includes a pre-authentication n procedure before the signature verification process. The one-way hash chain and a group rekeying technique are used in the pre-authentication procedure.

Manivannan et al.[10] reviewed studies on privacy, authentication, and secure message distribution on VANETs that had been published in the previous ten years. Based on the techniques and methodologies used in the publications, D. Manivannan et al. categorized the papers into many areas. D. Manivannan et al . compared and contrasted the techniques in each area, analyzing their pros and cons. Then D. Manivannan et al. spoke about some of the unresolved issues that needed to be addressed. D. Manivannan et al. believe that our survey will be a useful resource for other academics working in these fields, as well as help to address some of the remaining issues.

For VANET security. Ahamed et al. created unique anonymous mutual and batch authentication procedures[11]. To authenticate automobiles, the proposed system employs a number of well-known cryptographic algorithms. The security strength of our proposed system is tested against various security attacks in order to outperform previously revealed solutions. To assess the computational complexity of our proposed approach. Anis Begum Shakeel Ahamed et al. perform a lot of simulations.

It confirms that to reduce attacks on cars and network infrastructures, VANETs provide security services such as authentication, anonymity, privacy protection, message integrity, and others. Many research options have been developed in the past to address these security issues. In their study, some of the published works of literature are evaluated, which provide answers to security issues such as authentication and sequestered safety, and the solutions are contrasted to gain a better understanding.

3. Proposed system

To secure and prevent disrupting VANET connections, many authentication systems have been presented in the literature. “Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks” and “On-site Driver ID”: A secure authentication technique for vehicular ad hoc networks based on a new electronic device identity(EID) for local physical and online authentication in 2006. At the end of 2009, approx., 13 Mio Spanish citizens out of more than 46.5 Mio habitants were in procession of an eID cards are discussed in this part. This section demonstrates the VANET system paradigm, a potential dual authentication scheme, and key management

To safeguard the vehicle against unauthorized vehicle, we recommended first and foremost a Dual Authentication method. Second, they recommended using “a dual group key management procedure” to create or update a group key when a vehicle departs or joins a group.

3.1. VANET system model

The three essential components of the VANET system are the TA, RSUs, and OBUs installed on moving vehicles, as depicted in **Figure 1**. sensor networks in OBU are in each vehicle to gather data like breaking information, velocity and so on. Over the wireless channel, the collected data is transferred as messages to neighboring automobiles. Through a wired connection, all RSUs are connected to one another and, in turn, to the TA. The TA is in charge of the general operation of the VANET system.

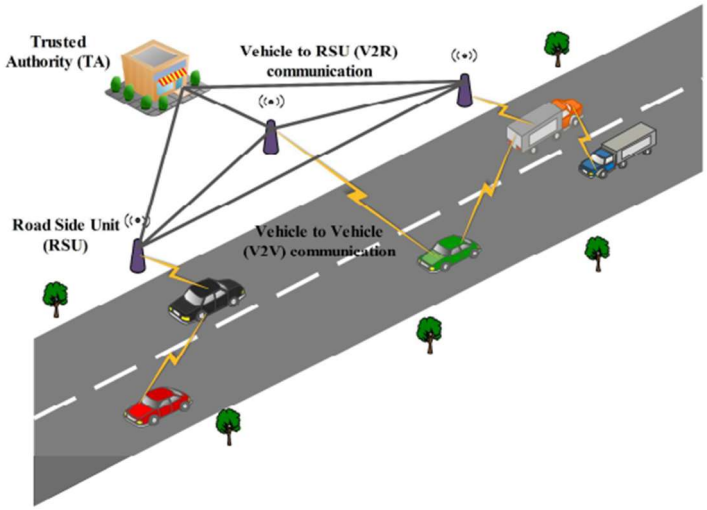

Figure 1. VANET system model.

TA: Vehicle users, vehicle OBUs, and RSUs must all be registered with TA. It’s also in charge of making sure that genuine OBU auto identification or user identities are recognized, in order to prevent fraudulent cars out of the VANET system. The TA is assumed with high computational power and sufficient storage capacity. In the instance of broadcasting harmful communications or engaging in malicious behavior, the TA has the authority to reveal the true identity of OBUs.

RSU: RSUs are usually stationary devices that are placed beside highways or in specialized sites such as parking lots or traffic intersections. A transceiver, antenna, CPU, and sensors are all found in an RSU, just as they are in an OBU. Automobiles are served by RSUs that are strategically located along highways. An RSU, for example, might be stationed at a road intersection to assist in traffic management and accident reduction. A directional antenna is used by an RSU to send a message to a specified location. The RSUs have the ability to store data from the OBU and TA of the vehicle.

OBU: The OBU on each vehicle is a transceiver that communicates with other vehicles' RSUs and OBUs, as well as a computational unit. The OBUs are powered by the car's battery.

Each vehicle features sensors such as a Travel Prediction-based Data forwarding(TPD), Global Positioning System(GPS) receiver, a speed sensor, an EDR and forward and rear sensors to provide information to the OBU. Vehicle's present location is collected by sensors. One of these pieces of equipment is the GPS receiver, which is utilized to give geographic information such as the vehicle's location. The TPD houses sensitive information such as the private key, group key, and vehicle identity. The Endpoint Detection and Response is a device that is used to record data from automobile accidents and collisions. The speed sensor records information like velocity and breaking. Over the wireless channel, all of this seen and gathered data is sent as messages to nearby automobiles.

3.2. Technique for dual authentication

The TA creates Vehicle Secret Keys (VSK1), which are issued to automobiles after the registration process is completed. When the automobile connects for the first time to the network, it utilizes the acquired VSKi to start the first authentication procedure. The authors proposed that this authentication procedure be carried out between the vehicle and the TA. N1,IDV1 (Vehicle ID1), and HC1 are the vehicle's VSK1 and sent in the following message:

$$(\{N1||\ HC1||\ IDV1\}\ \_\ VSK1||IDV1||IDTA1\ ||TS1\ ) \tag{1}$$

Following receipt of this transmission, the RSU adds IDRSU to its identity and the TA creates Vehicle Secret Keys (VSK1), which are issued to automobiles after the registration process is completed:

$$(\{\{\ N1||\ HC1||\ IDV1\ \}\_VSK1||\ IDV1||\ IDTA1||\ TS2||\ IDRSU1\}\_\ RSK1). \tag{2}$$

The TA decodes this message using Risk Security Keys (RSK1) rather than VSK1 when it gets it. The HC1 (Hash Code) acquired from the car is checked by TA1. If AC1 (Authentication Code) equals the locally determined HC1, where AC1 = SHA 256, the TA computes AC1 (Authentication Code) (HC1).

$$(\{\{AC1||\ IDV1||TS3||\ Lifetime\}\_TA-Pvt1||\ IDTA1\}\_VSK1||\ IDTA1\ \}\_RSK1) \tag{3}$$

Before transferring the message to the automobile, the TA sends it to the RSU1, which encrypts it with its RSK1.

When the authentication stage is completed, each vehicle should get AC1, which is preferred for communication.

3.3. Management of key

The Chinese Remainder Theorem can dynamically assist the trusted authorities (TAs) whilst generating and broadcasting new group keys to the vehicles in the network management phase. TA may produce two sorts of group keys: primary user groups (PUs) and supplemental user groups (SUGs).

The procedure of generating group keys in TA and on the vehicle side is explained shortly in Algorithm 1.

1) TA: TA performs the necessary initialization and key calculation, which includes the four phases listed below.

Algorithm 1 Group key management

1: Step (1): First, TA calculate $\partial g \prod_{(j=1)}^{m}(PUSKj)$.

2: Step (2): For j ∈ [1, n], TA calculate $xj = \frac{\partial g}{PUSKj}$.

3: Step (3): TA calculate yi such that $xj \times yj \equiv 1 \, mod \, PUSKj$.

4: Step (4): The medium value μ can be computes as = $\sum_{j=1}^{m} vari$, where vari = xj × yj .

Here ∂g represents the propagation speed of the vehicles, while step 3 is going to calculate the vehicles in the track.

At this stage, TA chooses the group key k pub as the primary user at random (PU). As a result, pub is created in accordance with the formula γpub = k pub × μ. Finally, information may be safely transferred to the car using the authentication mechanism mentioned above. In the same way, the secondary user (SU) group key ksug can be selected and computed.

2) Vehicle: Using the technique, the secret key k pub may be simply obtained from the received message k pub = pub mod PUSKj. As a result, main and secondary users are allocated the PUs group key k pub and the SUs group key ksug, respectively.

In VANETs, dual authentication security may be used to prevent unauthorized users from accessing the network. Furthermore, utilizing the Chinese Remainder Theorem (CRT), TA can complete the user join and revocation method with only a little quantity of user data, which is important in VANETs applications.

3.4. Performance evaluation

The total time necessary for dual authentication is the time it takes to complete all of the protocol's required authentications. We can see that they each have exactly four messages, approximately equal message lengths, and the same amount of entities (TA + RSU + Vehicle = three entities). As a result in **Table 1**, we've opted to simply compare them on the basis of total treatment delay under different scenarios, which may be calculated as follows:

$$D_{Treat} = D_{dec/enc\_SK} + D_{ash+Ddec/enc\_PvKh} + D_{Ddec/enc\_PbK} + D_{Dsig} \quad (4)$$

Table 1. Total treatment delay under different scenarios.

Technique	Total treatment delay (ms)
On-siteDriverID	0.46
Authentication Proposed method	0.06
Re-authentication Proposed method	0.032
Dual Authentication method	0.0311

Our suggested method, which is only utilized in the first connection of the car, minimizes recognition latency by up to 85% when compared to On-siteDriverID. Furthermore, our suggested re-authentication, which is performed every handover between two neighboring RSUs along the vehicle's journey, the authentication decreases latency by 94% and 55%, respectively. For this we can adopt On site Driver ID method (**Table 2**).

Table 2. Authentication delay under different scenarios.

Number of valid signatures	With pre-authentication	Without pre-authentication	No attack
60	146	187	246
80	181	239	286
100	219	279	328
120	257	321	373
140	291	359	419
160	326	401	474
180	359	438	528
200	398	481	598

In **Figure 2**, we examine the authentication delay in various cases. The absence of a Deniel of Service (DoS) assault is shown by the black star line. In scenarios where DoS assaults occur, with the total number of valid signatures, respectively, to demonstrate the scenarios with and without a pre-authentication procedure. We can observe from the attached little image in **Figure 3** that pre-authentication has little influence on authentication latency when compared to a situation without a DoS assault. In the event of a DoS attack, however, without pre-authentication, the authentication latency would be greatly altered. As a result, the proposed pre authentication approach can identify bogus signatures effectively. To put it another way, the suggested approach may successfully reduce DoS attacks on VANETs using signature-based authentication.

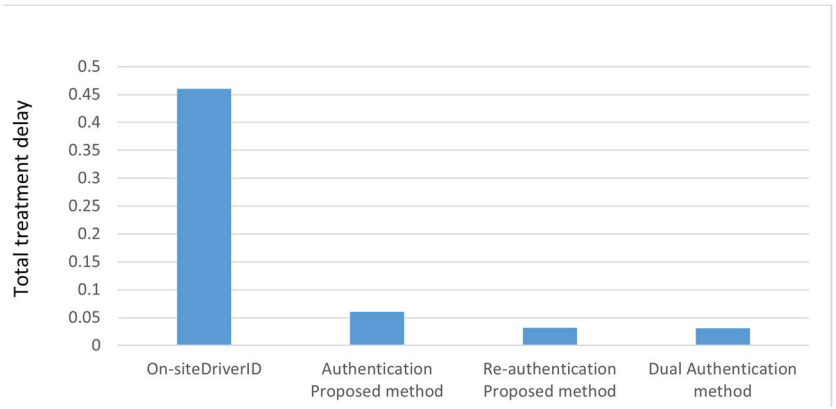

Figure 2. Total treatment delay under different scenarios.

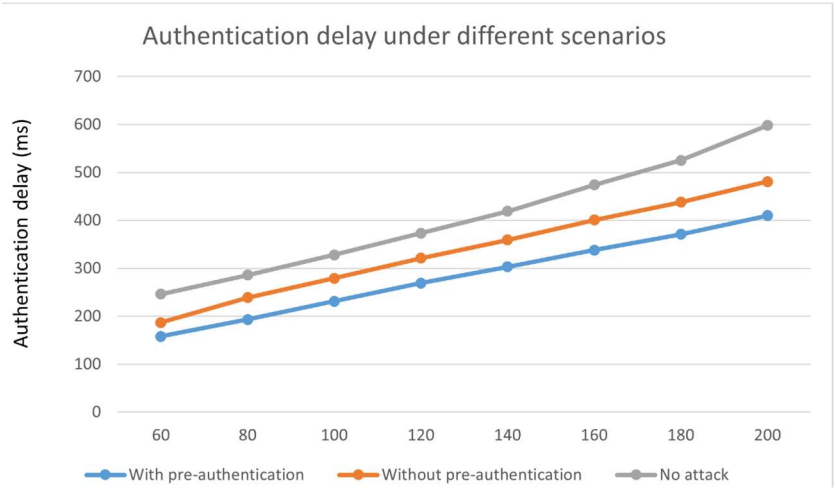

Figure 3. Authentication delay under different scenarios.

When compared to Dual Authentication, our suggested authentication provides more security and a shorter time. Furthermore, our often used suggested re-authentication provides the same level of security as our proposed authentication but with a very low latency that is about equivalent to the time required for Dual Authentication. Furthermore, our often used suggested re-authentication provides the same level of security as our proposed authentication but with a very low latency that is about equivalent to the time required for Dual Authentication.

4. Conclusion

We describe a dual authentication technique in this paper for maintaining high security on the vehicle, thereby prohibiting unauthorized automobiles from entering the VANET. Second, we find the most frequently occurring individual data on the server and expand it to larger and larger item sets, as long as those item sets appear frequently enough on the server. To efficiently distribute and update a group key to a group of users throughout their join and depart actions, a frequent data identification and dual group key management system is utilized. The suggested dual key management has the significant benefit of allowing users to be added or removed from the VANET group quickly and efficiently by altering a small amount of data. Our proposed method minimizes recognition latency by up to 85% when compared to On-site Driver ID. Furthermore, our suggested re-authentication, which is performed every handover between two neighboring RSUs along the vehicle's journey, decreases authentication latency in On-site Driver ID by 94%, while others are 55%.

Author contributions

Conceptualization, DK and RD; methodology, DK; software, DK; validation, RD and DK; formal analysis, DK; investigation, DK; resources, DK; data duration, DK; writing—original draft preparation, RD; writing—review and editing, RD; visualization, RD; supervision, RD; project administration, RD. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Rekik M, Meddeb-Makhlouf A, Zarai F, et al. Improved dual authentication and key management techniques in Vehicular Ad Hoc Networks. In: Proceedings of 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA); 30 October–3 November 2027; Hammamet, Tunisia. pp. 1133–1140. doi: 10.1109/aiccsa.2017.118
2. Azees M, Vijayakumar P, Jegatha Deborah L. Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems* 2016; 10(6): 379–388. doi: 10.1049/iet-its.2015.0072
3. Rekik M, Obaidat MS, Makhlouf A, et al. An optimized and secure authentication scheme for Vehicular Ad Hoc Networks. In: Proceedings of 2018 IEEE International Conference on Communications (ICC); 20–24 May 2018; Kansas City, MO, USA. pp. 1–6. doi: 10.1109/icc.2018.8422101
4. Vijayakumar P, Azees M, Kannan A, et al. Dual authentication and key management techniques for secure data transmission in Vehicular Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems* 2016; 17(4): 1015–1028. doi: 10.1109/tits.2015.2492981
5. Tan H, Choi D, Kim P, et al. Comments on "Dual authentication and key management techniques for secure data transmission in Vehicular Ad Hoc Networks." *IEEE Transactions on Intelligent Transportation Systems* 2018; 19(7): 2149–2151. doi: 10.1109/tits.2017.2746880
6. Priya MP, Jayaselvi P, Valarmathi R. A cooperative dual message authentication and group key management in VANET. *International Journal of Pure and Applied Mathematics* 2018; 118(18): 3721–3728.
7. Sayana SS, Bernald LM. Dual authentication and key management for secure transmission in Vanet. *International Research Journal of Engineering and Technology (IRJET)* 2018; 5(4): 3048–3051.

8. Greeshma TP, Roshini TV. A review on privacy preserving authentication in VANETs. In: Proceedings of 2018 International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT); 23–24 March 2018; Kannur, India. pp. 235–235. doi: 10.1109/iccpcct.2018.8574315
9. He L, Zhu WT. Mitigating DoS attacks against signature-based authentication in VANETs. In: Proceedings of 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE); 25–27 May 2012; Zhangjiajie, China. pp. 261–265. doi: 10.1109/csae.2012.6272951
10. Manivannan D, Moni SS, Zeadally S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs). *Vehicular Communications* 2020; 25: 100247. doi: 10.1016/j.vehcom.2020.100247
11. Ahamed ABS, Kanagaraj N, Azees M. EMBA: An efficient anonymous mutual and batch authentication schemes for VANETs. In: Proceedings of 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT); 20–21 April 2018; Coimbatore, India. pp. 1320–1326. doi: 10.1109/ICICCT.2018.8473110