International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

PRESERVING SECURITY AND INTEGRITY IN A VEHICULAR AD-HOC NETWORK USING PSEUDO ID-BASED SCHEME

Darshini Y[1] ,Dr. Jayasri B.S[2]

[1]M. Tech Scholar, [2]Associate Professor

Department of CSE, National Institute of Engineering, Manandwadi road, Mysuru.

Abstract: The rapid growth of Mobile Ad-hoc Network have triggered the Vehicular Ad-hoc network (VANET), for providing efficiency and traffic security on roads, as the schemes that are newly introduced can create new environment to drivers. in real time environment Vehicular communication can make privacy a real challenge, which in turn affects the large scale deployment of these issues. As of now many of the existing systems suffers from lack of insecurities, since the authentication with respect to their nodes is not properly secured and in case of large deployment of VANET ,privacy become difficult as the number of nodes get increases ..Hence it is more challenging to authenticate and preserve privacy in vanet. So ,Pseudo ID-Based authentication scheme is proposed, so that it reduces the issues regarding privacy and security and enhances the traffic safety and preserves vehicles privacy.

Keywords - Authentication, Privacy, Vehicular ad hoc network (VANET)

1.INTRODUCTION

The main aim of VANET is to provide road and traffic safety in means of transportation. Recently so many of the peoples lost their lives due to incorrect traffic messages that are passed on to their vehicles. In order to avoid this a VANET technology was introduced, which enhances the drivers safety on roads and avoids the road accidents. VANETs uses Pseudo ID-based scheme to provide authentication for the complete VANET operations like maintaining road safety messages and traffic related messages.in VANET infrastructure This scheme mainly consists of 3 components, which have their own set of operations:[1] The trusted authority ,[2] The road side unit and [3] the On board unit[4] Vehicles. Trusted authority is a main unit in the complete infrastructure, it holds the major responsibilities in the system.it accepts and stores the digital signatures that are issued by the RSU unit. The RSUs are located in roads which acts as the router, whose responsibility is to generate the digital signatures, RSUs are also a part of the system. while the OBU is a GPS-based tracking device that are equipped in every vehicle for sharing the vehicle information to RSUs and other OBUs. OBU takes input power from the car battery, and each vehicle consists of a sensor type global positioning system.

1.1 Problem Statement

VANET has their own set of challenges, particularly in the aspect of privacy and security. Because of the un-authenticated data which are shared over the network, the operations grants to malicious attacks and service abuses, which leads great threat to drivers. Furthermore, as an example of Mobile Ad hoc Network (MANET), the challenges and issues faced by MANET are inherent in VANET too. Moreover, VANETs are more challenging due to their high mobility and large scale deployment.

2. SYSTEM MODEL

The proposed network model consists of several blocks, which are treated as the nodes in the network infrastructure, the main components are: Trusted Authority (TA), Road side units (RSU) and the vehicles along with the Service Providers (SPs).The TA is the main entity in the Vanet network. TA is fully trusted, as it rolls out the major factors in the system ,also it is completely trusted by the other entities. TA provides sufficient computational and storage resources, in order to help the vehicles get register with it.

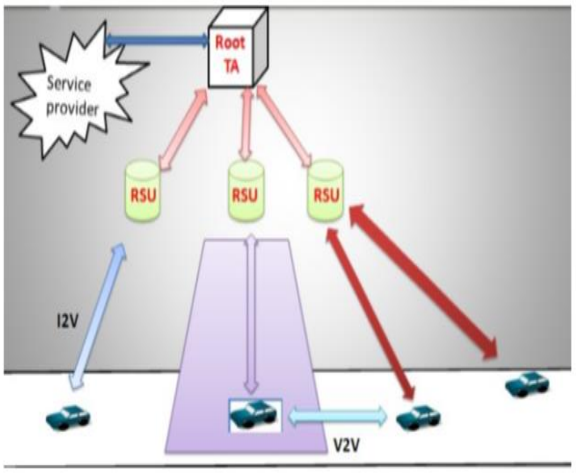

Fig 1: The typical vanet scenario

Fig 1.depicts the complete vanet scenario whereas, The TA is considered to be the trusted party it carries out certain tasks, as follows:1) It stores the digital signatures issued by RSU s 2) It takes control of vanet entities and provide proper signatures to intended and legitimate vehicles. Road side units are also the part of the network which also acts as the router, the infrastructure supports vehicle to communicate with other vehicles. RSU is responsible for maintaining the communication of all the OBUs within its range. OBUs the On-Board Units are the radio devices that are installed on every vehicle, which helps to broadcast traffic related messages, emergency warnings and the road-safety messages. Each OBU consists of the Tamper Proof Devices (TPD) which is accountable for storing the secret messages and parameters which also implements the cryptographic operations. This device hides all the essential operations, it masks the real identity of the vehicles, by portraying the pseudo identity making the attacker impossible to hack the real identity of the vehicle thus ,it becomes difficult for hacking.

3.PROPOSED PSEUDO ID-BASED SCHEME

In this section, The Pseudo Id-based scheme is introduced to protect the security and integrity in the VANET network. The scheme mainly has six phases: (A). Initially a vehicle requests the nearest RSU for the service, by sending the "joining request" message, at this point the RSU opens the session with TA to check the legitimacy of the particular vehicle. (B). once the vehicle is verified as trusted it receives the digital signature from the RSU, it browses for the file, encrypts it and starts the broadcasting operations. (C).If RSU comes to know that the vehicle is not legitimate, its confirmed that, there is a presence of intruder who are trying to grab the confidentiality of the network. (D) After which the RSU informs about the attacker to

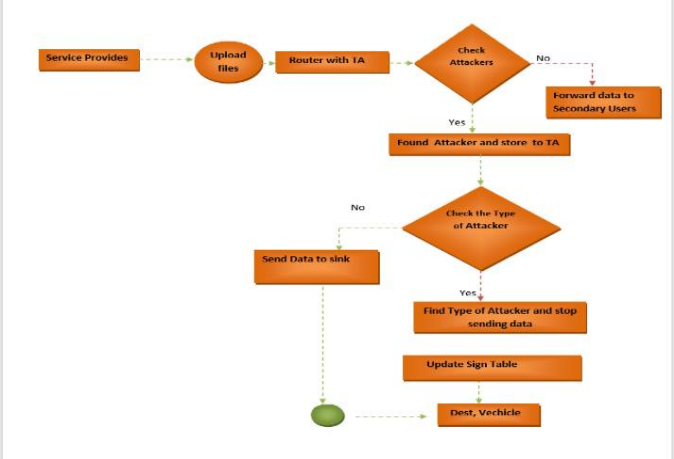

Fig 2: Data flow diagram

The TA and thus TA by estimating the kind of a attacker it stops sending data to them.(E) The RSUs gives the "warning message" about the intruder to the vehicles within its range.(F)As the OBUs are installed in every vehicle which also consists of TPDs, it makes attackers difficult steal the vehicle information by portraying pseudo id of the vehicle instead if real identity. Fig 2 briefs the working flow through data flow diagram, it explains the initial stages and the different cases of the project.

4.IMPLEMENTATION AND RESULTS

We run this project in the Eclipse Galileo, to evaluate the performance of our scheme in terms of privacy and authentication. The main aim of the project is to avoid illegal messages that causes serious impact on road-safety, when the vehicle enters the management it gets registered with the nearest RSU, when service provider receives the joining request from the vehicle RSU checks for the legitimacy once it is verified ,the SP browses the file and send it to receiver through Message authenticated code(MAC) address, it's the path created to exchange message between service provider, router and the receiver. If a vehicle is found non-legitimate it is dropped, and RSU stops sending the data. As compared to any another scheme the pseudo ID-based provides high security and privacy for the vehicles, it requires only minimum storage, for communication and storing the data and hence reduces the computational costs.

4.1 Test Cases and Results

The purpose of Testing is to discover errors and flaws, testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, assemblies, sub-assemblies and/or a finished product. The various types of test cases and results are as follows:

Table 1:Test cases with their results

Test ID	Test Cases	Expected Output	Actual Output	Status
1.	Assigns Details to vehicles	Digital signatures are created for all the vehicles	Vehicles will have their own digital signatures	Pass
2.	Validity of Digital Signatures	Digital signatures will have their validity	The Digital signatures can be used with validity	Pass
3.	Browse for the file	File is fetched from folder	File is ready for Encryption and Decryption	Pass
4.	Requests the Digital Signature	Request the digital signature of particular vehicle	Requested Digital signature is issued	Pass
5.	Encrypts and uploads the file	The router is selected to which it has to send the data	Data is passed through MAC to intended vehicle	Pass

5. CONCLUSION

This paper proposes a new pseudo-ID-based scheme for a VANET to provide conditional anonymity and integrity. The proposed scheme satisfies all the security and privacy requirements of a VANET by using pseudonym instead of the real identity, and as well as resists the common attacks. Our scheme can provide conditional anonymity in which only the real identity of a vehicle conducting malicious activity is revealed. We were able to overcome the previous drawbacks of ID-based schemes, and our scheme does not require the complex operations that are produced by a bilinear pairing operation. It can also preserve privacy in terms of the vehicle's real identity, even from an insider attacker.

6.FUTURE WORK

The TA can trace a bogus vehicle and revoke it as a member of the VANET. A security analysis shows that our scheme is secure under the random oracle module and can meet the security and privacy requirements of a VANET. We compare our scheme with recent proposed ID-based schemes and show that it has computation costs that are lower than previous schemes and lightweight communication. Our scheme resolves these challenges positively and is suitable for VANETs.

7.REFERENCES

[1] D. Lloyd. 2016. *Reported Road Casualties in Great Britain: Main Results 2015*. [Online]. Available: https://www.gov.uk/government/statistics/reported-road-casualties-in-great-britain-main-results-2015

[2] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, ``A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom Filters,'' *ICT Express*, vol. 4, no. 4, pp. 221_227, Dec. 2017.

[3] Y. Ming and X. Shen, ``PCPA: A practical certi_cateless conditional privacy preserving authentication scheme for vehicular ad hoc networks,' *Sensors*, vol. 18, no. 5, p. 1573, May 2018.

[4] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, ``VANET security surveys,'' *Comput. Commun.*, vol. 44, pp. 1_13, May 2014.

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ``Vanet security challenges and solutions: A survey,'' *Veh. Commun.*, vol. 7, pp. 7_20 Jan. 2017.

[6] J.-P. Hubaux, S. Capkun, and J. Luo, ``The security and privacy of smart vehicles,'' *IEEE Secure. Privacy*, vol. 2, no. 3, pp. 49_55, May 2004.

[7] M. Raya and J.-P. Hubaux, ``Securing vehicular ad hoc networks, ''*J. Comput. Secure.*, vol. 15, no. 1, pp. 39_68, Jan. 2007.

[8] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, ``ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications, ''in *Proc. 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 1229_1237.

[9] 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.

[10] U. Rajput, F. Abbas, and H. Oh, ``A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET,'' *IEEE Access*, vol. 4, pp. 7770_7784, 2016.