ISSN No. 0976-5697

Volume 6, No. 6, July - August 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Survey on Efficient Secured data Transmission for MANET

Rasika Kiranchandra Nerkar
Department of Computer Science and Engineering
Nagpur Institute of Technology ,Nagpur

Abstract: Virtually in all facets of modern life transportation systems play a major role . However, important challenges remain in further improving their efficiency and safety and in developing value-added applications .MANET will be an application developed for finding all online users and then make a group of people that are within some range of distance and for that we provide some parameters like latitude & longitude (Indicate the location & position).

The MANET application will involve a GPS Tracker for Calculating the Latitude & Longitude and that latitude & longitude are take as Input in the application. After that the users who are in same range of distance can communicate with each other by means of sending messages to each other and ask each other for any help. This application will also provide the security by hiding the identity of the users communicating with each other by means of messages and the person who are communicating.

Index Terms – GPS Tracker ,Latitude , Longitude ,security.

I. INTRODUCTION

On road safety of the vehicles equipped with wireless devices can be improved with the help of Vehicular Ad Hoc Networks as such can devices can build a Vehicular Ad Hoc Network where vehicles' the On-Board Units can communicate with other vehicles' OBUs or fixed infrastructure called Road Side Units[1]. VANETS can be regarded as an important development to achieve automatic and dynamic information collection applications as they become available[6].

Vehicles have to rely on On-Board Units so that these applications operate reliably and securely, in order to broadcast their messages and also to verify the received ones[7]. For secured communication, IEEE 1609.2 standard has proposed use of Elliptic Curve Digital Signature Algorithm so that the signatures verify messages, which could cause high computational overhead on the standard OBU hardware[2].

According to the Dedicated Short Range Communications , each vehicle will broadcast a traffic safety message in every 100-300 milliseconds to the other vehicles and this message will contain the vehicle's driving related information, as location, speed etc[5]. However, an attacker may deliberately send a large number of signatures which are invalid that a receiver may take much long time to process and may eventually lead to Denial of Service (DoS) attacks. However, these attacks can be also initiated without desire of any harm . For example, in case a particular vehicle receives more than the specified number of messages in its radio range, it is not possible to do the verification of all the messages that are sent 5 times per second before their deadline and hence the attackers can easily destroy a VANET.

Many of the existing [3]-[5] mechanisms use the identity based batch verification scheme so that they can avoid the attacks caused by DoS . Moreover, the main focus is on the communication between the vehicles and the RSUs as the computation costs of verifying the signatures are dominated by the operations of the pairing and point multiplication over the elliptic curve are costly for OBUs. TESLA provides a good alternative to these signatures [9] , [10] as it makes use of the symmetric cryptography with the delayed release of keys.

As symmetric cryptography is much more faster than the signatures, TESLA is more resistant to DoS attacks and it is therefore applied for vehicle-to-vehicle communication .

However, the drawback of TESLA is that the receiver has to buffer the packets during single disclosure delay before they are authenticated. This would not actually be practical for the applications where the receiver requires to verify urgent messages quickly. Since TESLA is not able to provide the non-repudiation property , we cannot completely give up digital signatures. Hence , another more flexible scheme VSPT , VANET authentication with Signatures and Prediction-based TESLA has been proposed so that a wide range of properties can be provided for authentication .

II. LITERATURE REVIEW

Table: 1

Sr. no.	Title	Year of Publishing	Facts and findings
1.	Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective.	2006	Given a large number and diverse nature of applications, it is favourable to develop a classification method in order to facilitate the VANET research. Our study goes through two main steps i.e. classification and characterization. Firstly, we focus on a rich set of representative applications and characterize them w. r. t probable application and networking-related attributes. The characterization process fosters understanding of the applications and also sets the stage for the classification as it reveals numerous sharing of application features.
2.	Flooding-resilient broadcast authentication for VANET.	2011	In this paper, two efficient broadcast authentication schemes, Fast Authentication (FastAuth) and Selective Authentication (SelAuth), two counter measures to signature flooding have been proposed. FastAuth secures periodic messages by exploiting the sender's ability to predict its future beacons, FastAuth also enables 50 times faster verification than the previous mechanisms by making use of Elliptic Curve Digital Signature Algorithm. SelAuth secures multi-hop applications in which a fraud signature may spread out easily and quickly and impact a significant number of vehicles. It provides fast isolation of malicious senders, even under a dynamic topology, and consumes only 15%–30% of the computational resources as compared to the other schemes.
3.	An efficient identity based batch verification scheme for vehicular sensor networks.	2008	In this paper, an efficient batch signature verification scheme for communications between vehicles and RSUs has been given. Here, an RSU can verify multiple received signatures at the same time such that the total verification time will be reduced.
4.	BAT: A robust signature scheme for vehicular networks using binary authentication tree.	2009	In this paper, an efficient and robust signature scheme for vehicle-to-infrastructure communications, called binary authentication tree (BAT) has been proposed. This scheme can effectively eliminate the performance bottleneck while verifying a number of signatures within a strictly required interval and also under adverse scenarios with bogus messages. The scheme can also be easily transplanted to other similar schemes. In addition, it also offers the other conventional security for vehicular networks, such as traceability and identity privacy.
5.	ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks.	2011	In this paper, an anonymous batch authenticated and key agreement (ABAKA) scheme for authentication of multiple requests sent from different vehicles and establishment of different session keys for different vehicles at the same time has been introduced .

III. PROPOSED WORK

Our approach is to solve the problem in existing system by providing strong authentication scheme and also to provide efficient cryptography algorithm which we will provide security over that and for providing authentication we have applied three levels of authentication by providing login id followed by QR code and lastly the image authentication. Moreover we have also provided authentication on the server side.

Our main objective is to provide security. For that we implement a server, and server monitor's all activity that user will do. For security we are going to encrypt the conversion that will take place between the users by using Advanced Encryption Standard scheme. This scheme will encrypt the messages and hence maintain the security constraints.

We also provide a unique id to all users so that the privacy of the users is preserved and hence he can communicate with anyone within the intended range and get the desired help in case of emergency.

IV. CONCLUSION

In our work, we will analyze the security requirements of authentication for vehicle-to-vehicle communication in the Mobile Ad Hoc Networks. We will make the use of Advanced Encryption scheme for the encryption of electronic data and provide higher security for the authentication of messages and also preserve the end users privacy .

V. REFERENCES

[1]. F. Bai, H. Krishnan, V. Sadekar, G. Holland, and T. Elbatt, "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective," in Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet), 2006.

[2]. H. C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Flooding-resilient broadcast authentication for VANETs," in Proceedings of ACM Mobicom'11, pp. 193-204, Sep. 2011.

[3]. C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," in Proceedings of IEEE INFOCOM, pp. 816-824, 2008.

[4]. Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," IEEE Transactions on Wireless Communications, vol. 8, no. 4, pp. 1974-1983, Apr. 2009.

[5]. J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks, " IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248-262, Jan. 2011.

[6]. F. Wang, D. Zeng, and L. Yang, "Smart cars on smart roads: an IEEE intelligent transportation systems society update," IEEE Pervasive Computing, vol. 5, no. 4, pp. 68-69, 2006.

[7]. IEEE Standard 1609.2 - IEEE Trial-use standard for wireless access in vehicular environments - Security services for applications and management messages, July, 2006.