ISSN:0975-9646

A Survey on Efficient and Secure data transmission for MANET

Ms. **Rasika Nerkar**
Department of Computer Science and Engineering
Nagpur Institute of Technology ,Nagpur

Mr**. Jagdish Pimple**
Assistant Professor
Department of Computer Science and Engineering
Nagpur Institute of Technology ,Nagpur

Abstract-Vehicular Ad Hoc Networks enables a fast and efficient vehicle-to-vehicle communication and also enhances road safety to improve driving experience. In order to secure periodic single-hop beacon messages in case of these important security approaches. At the same time, it is exposed to the possibility of being attacked as excessive signatures would exhaust the computational resources of the vehicles. Several approaches are discussed in this paper. An authentication mechanism, VANET authentication with the help of kerberos which will provide a five level security including password , captcha , image recognition etc. Since we cannot show the real vehicle-to-vehicle communication we would make use of mobile phone to show the communication in the form of a MANET.
This mechanism enables fast and efficient verification of messages by keeping the identity of the sender private.

Keywords—VANET, signatures, beacons, authentication, MANET , kerberos.

1.INTRODUCTION

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

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

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

Most of the existing [3]-[5] mechanisms make use of identity based batch verification scheme in order to avoid the DoS attacks. However, the focus is mainly on the communication between vehicles and RSUs as the computation costs on verifying the signatures dominated by the operations of pairing and point multiplication over the elliptic curve are expensive for OBUs. TESLA provides an efficient alternative to signatures [9] , [10] by making the use of symmetric cryptography with delayed release of keys.

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

TESLA has a drawback that the receiver has to buffer packets during one disclosure delay before they are authenticated. This would not be practical for those applications where the receiver requires to verify the urgent messages immediately. Since TESLA is unable to provide the non-repudiation property , we cannot give up digital signatures. Therefore, another more flexible scheme VSPT, VANET authentication with Signatures and Prediction-based TESLA is proposed in order to provide a wide range of properties for authentication.

2. LITERATURE SURVEY

[1] "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective" by F. Bai, H. Krishnan, V. Sadekar, G. Holland, and T. Elbatt
Most of the applications have been identified by the automotive community. Given the large number and diverse nature of various applications, it is favourable to develop a classification method in order to facilitate the future VANET research. We present a study that 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. Thus, we have categorized applications into various classes, with the view of balancing the trade-off between exploiting as many application similarities as possible as well as preserving their differences. This is of utmost importance to promote performance analysis for the newly designed rules.

[2] “Flooding-resilient broadcast authentication for VANET” by H. C. Hsiao, A. Studer , C. Chen , A. Perrig , F. Bai , B. Bellur, and A. Iyer
Digital signature is one of the important security primitive in Vehicular Ad-Hoc Networks since they provide authentication and non-repudiation in broadcast communication. The current broadcast authentication standard is exposed to the probability of being attacked by signature flooding in which excessive signature verification requests exhausts the computational resources of victims. In this paper, two efficient broadcast authentication schemes, Fast Authentication (FastAuth) and Selective Authentication (SelAuth), two countermeasures 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.It is used for single hop beacon messages whereas SelAuth secures multi-hop applications in which a fraud signature may spread out easily and quickly and also 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" by C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen
The adoption of state-of-the-art telecommunication technologies for collecting and sensing traffic related information, Vehicular Sensor Networks have been emerged as an application scenario that is vizualised to revolutionize the human driving experience and also the traffic flow control systems. In order to avoid any possible malicious attack and resource abuse, is widely recognized to employ a digital signature scheme as one of the most effective approach for VSNs to achieve validity , authentication and integrity. However, as the number of signatures received by a Roadside Unit (RSU) increases, a scalability problem emerges immediately, where it would be difficult for the RSU to sequentially verify each received signature within 300 ms interval as per the current Dedicated Short Range Communications broadcast protocol. 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" by Y. Jiang, M. Shi, X. Shen, and C. Lin
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" by J. L. Huang, L. Y. Yeh, and H. Y. Chien
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 . In vehicular ad hoc networks the speed of a vehicle is changed from 10 to 40 m/s (36-144 km/h); therefore, need for efficient authentication is necessary. As compared to the current scheme, ABAKA can efficiently authenticate multiple requests by a single verification operation and also negotiate a session key with each vehicle by broadcasting one message . Elliptic curve cryptography has been adopted in order to reduce the verification delay and also the transmission overhead and the security of ABAKA is based on the elliptic curve discrete logarithm problem . A detection algorithm has been proposed to deal with the invalid request problem, which may led to the batch verification failure.

3. PROPOSED WORK

Vehicular adhoc network is a very useful network for the safety of vehicles on road . One can communicate with other vehicles in case of an accident , losing the correct path etc through exchanging messages from one vehicle to another . In our project we will develop a manet network since it is possible to show its working practically .

The objective of this project is to form a secure network and for proving a secure network we will provide high authentication levels .We will also preserve the identification of the end user . The users will be able to communicate with each other by exchanging messages . In our application the user will easily be able to see the nearby (at the range of 5km) users so that instant help is possible in case of emergency .The purpose of preserving the identification is that sometimes there are Higher authorities i.e. ministers travelling through the raod so in that case we cannot reveal their identity.

4. CONCLUSION

In this work, we analyze the security requirements of authentication for vehicle-to-vehicle communication in Mobile Ad Hoc Networks. We make use of Advanced Encryption scheme i.e. AES for the encryption of electronic data and also provide higher security levels for the authentication of messages while preserving the end users privacy .

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.