International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 8 – JULY 2018.

ENHANCED IDENTITY BASED CRYPTOGRAPHY FOR SECURE AND SMART TRANSPORTATION IN VANET

CHARUNAYANA V[#1]

[#] *Assistant Professor, Department of Computer Science and Engineering , Vidyavardhaka College of Engineering, Mysuru, India*

***Abstract*— Vehicular Sensor Networks (VSNs) have emerged as a new application scenario that is envisioned to revolutionize the human driving experiences and traffic flow control systems. To avoid any possible malicious attack and resource abuse, employing a digital signature scheme is widely recognized as the most effective approach for VSNs to achieve authentication, integrity, and validity. However, when the number of signatures received by a Roadside Unit (RSU) becomes large, a scalability problem emerges immediately, where the RSU could be difficult to sequentially verify each received signature within 300 ms interval according to the current Dedicated Short Range Communications (DSRC) broadcast protocol. In this paper, we propose an enhanced Identity based cryptography which operates on batch based message verification system. It is been perceived that RSUs can receive multiple messages at particular time period which paves a way for modifying the messages. Initially, pseudo identifier is followed for each user and then the messages are signed and verified by the trusted authority. Experimental results have shown the efficiency of proposed IBC in terms of better transmission overhead and verification delay.**

***Index Terms*— VANET, Road side units, Onboard units, Identity based systems and Delay.**

I. INTRODUCTION

Nowadays, vehicles are equipped with high-technology devices, such as: GPS navigators, radars, and on-board units (OBUs). These wireless-enabled devices make vehicles intelligent and able to communicate with each other, and thereby form a self-organized vehicular ad-hoc network (VANET) [1]. Most proposed system architectures for VANET need to equip vehicles with a box that contains a radio interface to enable wireless communication between vehicles. The rapid mobility and dynamically changing topology of VANET cannot use the current IEEE wireless protocols 802.11 in its present state, so a modified version named 802.11p was developed by IEEE for vehicular networks. The modifications were mostly done in the MAC layer. Many wireless technologies like: a) IEEE 802.11p that is a standard for Dedicated Short Range Communication, DSRC, a Wifi type called Wireless Access in Vehicular Environment, WAVE, b) General Packet Radio Service (GPRS), c) IEEE 802.16 that is a standard for WiMAX, and d) 4G-Long Term Evolution (LTE) have been proposed for reliable vehicular communications.

Besides that, VANETs are always looked upon as systems that would open innovative and path breaking applications. Also, before the real technology hits the road, a series of detailed research is carried out around the world to make the system reliable and robust. In addition, VANETs are a promising area for the creation of Intelligent Transportation Systems (ITS) that provide assistance to drivers to increase their safety and comfort by offering useful services to them. Moreover, VANET is a kind of network that has two main types of communication: V2V and V2I, which are vehicle–to–vehicle and vehicle–to–infrastructure respectively. The set of applications that offer comfort and convenience-based services are referred to as non-safety applications, while the safety applications are more concerned with life-saving services [2]. With the assistance of V2V and V2I communications, potentially fatal road accidents can be avoided; dangerous driving behaviors can be alerted; city traffic flows can be optimized; and traffic jams can be alleviated. However, since vehicular communication systems (VCS) aim to serve people, any small error as unauthorized modification of data or system malfunction can be fatal.

Furthermore, VANETs command a unique grade of requirements to maintain liability and accountability of drivers involved in accidents, traffic violations, emission norms and irregularities in order to take punitive actions if a driver commits any crime. Besides that, location and context-aware services require pin-point user location and preferences to provide the most specific, exact and comprehensive list of personalized information. Despite that, communication of such information raises significant privacy issues that cannot be neglected. Also, privacy concerns in vehicular communications are necessary to provide protection for the user data from profiling and tracking. For example, location-based service applications have a high probability of privacy breaching and jeopardizing security-related issues [3], which decrease the widespread of VANET. Moreover, quality and privacy are two divergent tendencies that exist with VANET applications and have undeniable importance to the user [4].

The rest of the paper is organized as follows: Section II describes related work; Section III presents the proposed work; Section IV presents the experimental results and finally, concludes in Section V.

II. RELATED WORK

This section presents the related work of the study. Because the random oracle model is quite controversial, an important

open problem after the construction of the Boneh-Franklin scheme was to develop an identity based encryption scheme which is provably secure in the standard model. As a first step towards this goal, In [5], studied an identity based encryption scheme which is provably secure without random oracles, although in a slightly weaker security model. In this weakened model, known as selective identity security, an adversary needs to commit to the identity he wishes to attack in advance. In the standard identity based model, the adversary is allowed to adaptively choose his target identity. The security of the scheme depends on the hardness of the DBDH problem and the construction is quite inefficient. As an improvement, in [6] studied two efficient identity based encryption schemes, both provably secure in the selective-identity model and also without resorting to random oracle methodology. The first system can be extended to an efficient hierarchical identity based encryption system (see next section) and its security is based on the DBDH problem. The second system is more efficient, but its security reduces to the nonstandard DBDHI problem.

A later construction due to [7] is proven fully secure without random oracles. Its security reduces to the DBDH problem. However, the scheme is impractical and was merely given as a theoretical construct to prove that there indeed exists fully secure identity based encryption schemes without having to resort to random oracles. Finally, in [8] improves on this result and constructs a modification of the scheme which is efficient and fully secure without random oracles. Its security also reduces to the DBDH problem. The concept of hierarchical identity based encryption was first introduced by [9]. In traditional public key infrastructures there is a root certificate authority, and possibly a hierarchy of other certificate authorities. The root authority can issue certificates to authorities on a lower level and the lower level certificate authorities can issue certificates to users. To reduce workload [10], a similar setup could be useful in the setting of identity based encryption. In identity based encryption the trusted party is the private key generator. A natural way to extend this to a two-level hierarchical based encryption is to have a root private key generator and domain private key generators. Users would then be associated with their own primitive identity plus the identity of their respective domain, both arbitrary strings [11].

The first hierarchical identity based encryption scheme with an arbitrary number of levels is given by [12]. It is an extension of the Boneh-Franklin scheme and its security depends on the hardness of the BDH problem. It also uses random oracles. Boneh and Boyen managed to construct a hierarchical based encryption scheme without random oracles based on the BDH problem [13], but it is secure in the weaker selective-ID model [14]. In the aforementioned constructions, the time needed for encryption and decryption grows linearly in the hierarchy depth, thus becoming less efficient at complex hierarchies. In [15] presented hierarchical identity based encryption system in which the decryption time is the same at every hierarchy depth. It is selective-ID secure without random oracles and based on the BDHE problem.

III. PROPOSED WORK

This section presents the proposed model of our study on secured and safe smart transportation in VANET. The proposed pre-requirement composes of four steps, namely,

A. System Model:

The VANET model composes of four entities, namely, trusted authorities, application servers, Road Side Units (RSU) and Onboard Units (OBU). Each unit serves their functionalities. RSUs placed at lower layer of vehicles. Transport Layer Security (TLS) protocol is deployed between trusted authorities and applications servers. The messages are communicated only when the vehicles are authorized. By doing so, we achieved integrity of the messages. Then, signatures of the messages are responsible for verifying the messages.

B. Adversary Model:

Initially, let us assume that RSUs and OBUs are not trustworthy since the channels are not secured. Due to this scenario, the actions performed by adversaries are the:

i) Chance of message modification, illegitimate vehicles can modify the messages or destruction of infrastructure.
ii) Identity of the users can also be modified.

a) Security model:

The major security goals are the:

i) Authentication of messages: RSUs should consistently verify whether any message modification is there or not.
ii) Privacy of the users: Each identity of the users should be uniquely identified.
iii) Traceability: The actions performed by vehicles should be consistently checked for restricting anonymous vehicles.
iv) Unlinkability: By linking anonymous messages, the identity of user can steal.
v) Non- Repudiation: Due to wrong message broadcasting, the vehicles can insert onto the normal network.

The proposed phases are as follows:

1) Key Generation & Pre-distribution:

In our system, trusted authority is used for maintaining the identity of the vehicles. Based on user's details, the private keys are generated. Concurrently, the security parameters are initialized for RSU and OBU. Initially, the security parameters are initialized using identity groups G. A bilinear map G: G1 *G2 is formed as multiplicative group. Using this group, the TA randomly generates private and master key and then tampered on the vehicles. Similarly, RSU with public parameters such as { G, Gt, q, Pub1 and pub 2}. Therefore, an adversary cannot take advantages of the tamper-proof device even if the vehicle is stolen.

2) Pseudo Identity Generation:

In order to achieve privacy of the vehicles, pseudo identities are generated based on Identity based cryptography. Most of the system makes use of access control model for preserving the privacy of the vehicles. A vehicle inputs its unique real identity RID and the password PWD to initiate the device, where the PWD can be the signature of the RID signed by the TA. If the RID and PWD successfully pass the verification of the authentication module, the RID is delivered to the next module, the pseudo identity generation module. Otherwise, the device denies providing services for the vehicle. Obviously, the

authentication module enhances the security of the tamper-proof device since a malicious adversary cannot take advantages of it even though the tamper-proof device is physically held by the adversary.

3) Message Signing:

When vehicles are travelling on road, it periodically updates the traffic details to its intended network. To ensure the integrity of the messages, each message sent by a vehicle should be signed and verified when being received. The proposed sign-in process are as follows:

i) Each vehicle's message is denoted by M.
ii) Pseudo identity of the vehicles is also verified with private key pk1, pk2…pkn.
iii) With the help of private key, the signature of the message is generated.
iv) The vehicles with private key pk, and signature message SM passed onto the RSU system.

Furthermore, since all the messages are signed with different pseudo identities, thus none of the two messages can be connected to a single vehicle with the IBV signature scheme, which is expected to successfully address the issue of privacy preservation in VANETs.

4) Batch Verification:

Based on the network architecture as described in Section II, once an RSU receives a traffic related message from a vehicle, the RSU has to verify the signature of the message to ensure that the corresponding vehicle is not attempting to impersonate any other legitimate vehicle or disseminating bogus messages, which may result in tremendous impairment. Thus, this batch verification can dramatically reduce the verification delay, particularly when verifying a large number of signatures.

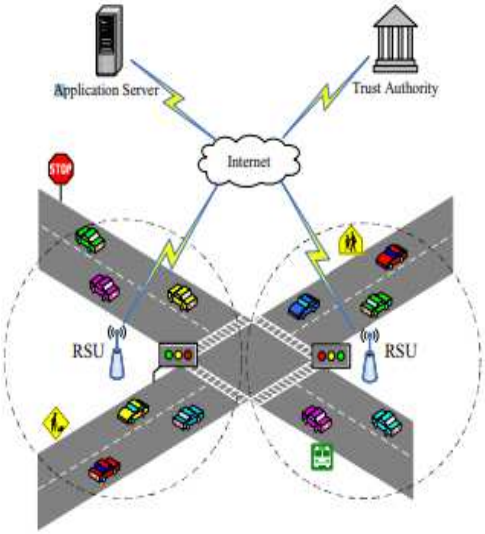

Fig.1. VANET- System Model

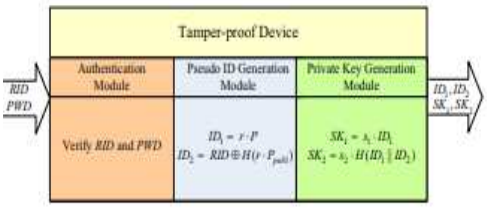

Fig.2. Developing trusted environment

IV. EXPERIMENTAL RESULTS

This section presents experimental analysis of the proposed identity based cryptography for achieving secured VANET environment. Since, we have assumed that all vehicles travel via RSU. The performance of the study is presented with Elliptic curve process as follows as:

A. Delay in Verification:

Let us compute time cost taken for performing cryptographic operations. In this process, time taken for multiplication point and pairing operation are computed using signature generation process. The fig.3 presents the delay in verification between proposed IBC and EC. It shows that proposed IBE performs better than existing elliptic curve.

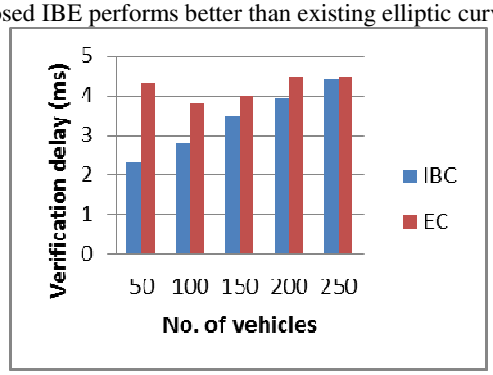

Fig.3. Verification delay

B. Transmission overhead:

The transmission overhead is studied under two aspects: he transmission overhead incurred by delivering the messages from a vehicle to an RSU, and the overhead incurred by delivering a message from an RSU to an application server. Since, the messages are signed and verified, the no. of bytes taken by proposed IBC is lesser than existing EC. Obviously, as the number of messages increases, the transmission overhead increases linearly. On the other hand, since no certificate for each message is required in IBV, the advantage gained in the proposed scheme is obvious. The fig 4 presents the transmission overhead between proposed and existing schemes.

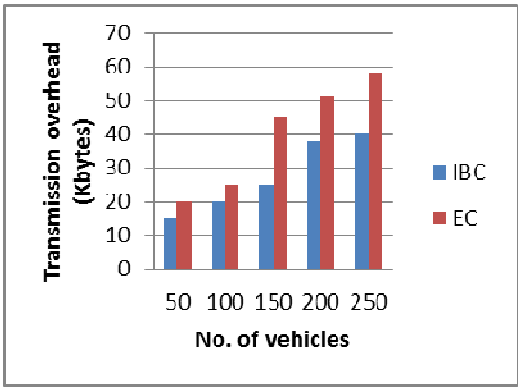

Fig.4. Transmission overhead between proposed and existing schemes.

V. CONCLUSION

In this paper, we have proposed an enhanced Identity Based Cryptography (IBC) which specifically senses the messages in VANET environment. Security and privacy of the VANET messages are a challenging task. In particular, the

proposed IBC scheme can significantly improve the system performance by fully taking advantages of verifying multiple message signatures at once instead of the verification of one after the other. Our scheme has also addressed the identity privacy and traceability issues in vehicular networks, where the signature of a message is signed according to a pseudo identity pair and private keys that are generated by the tamper-proof device. Furthermore, the IBC scheme enables the Trusted Authority (TA) to retrieve the real identity of a vehicle from any message signature, such that conditional privacy preservation can be achieved. Experimental results have shown the efficiency of proposed IBC in terms of better transmission overhead and verification delay.

REFERENCES

[1] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, A secure authentication scheme for VANETs with batch verification, Wireless Networks, vol. 21, no. 5, pp. 1733– 1743, 2015.

[2] D. He, S. Zeadally, B. Xu, and X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Trans. on Information Forensics and Security, vol. 10, no. 12, pp. 2681–2691, 2015.

[3] S. V. Miller, Use of elliptic curves in cryptography, in Conference on the Theory and Application of Cryptographic Techniques, 1985, pp. 418–426.

[4] N. P. Smart, The discrete logarithm problem on elliptic curves of trace one, Journal of Cryptology, vol. 12, no. 3, pp. 193–196, 1999.

[5] S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, b-SPECS+: Batch verification for secure pseudonymous authentication in VANET, IEEE Trans. on Information Forensics and Security, vol. 8, no. 11, pp. 1860–1875, 2013.

[6] D. He, N. Kumar, H. Shen, and J.-H. Lee, One-tomany authentication for access control in mobile pay-TV systems, SCIENCE CHINA Information Sciences, vol. 59, no. 5, pp. 1–14, 2016.

[7] J. Zhang, M. Xu, and L. Liu, On the security of a secure batch verification with group testing for VANET, International Journal of Network Security, vol. 16, no. 5, pp. 355–362, 2014.

[8] X. Boyen and L. Martin, Identity-based cryptography standard (IBCS): Supersingular curve implementations of the BF and BB1 cryptosystems, No. RFC 5091, 2007.

[9] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato, Internet X. 509 public key infrastructure time-stamp protocol (TSP), http://tools.ietf.org/html/rfc3161, 2001.

[10] N.-W. Lo and J.-L. Tsai, An efficient conditional privacypreserving authentication scheme for vehicular sensor networks without pairings, IEEE Trans. on Intelligent Transportation Systems, vol. 17, no. 5, pp. 1319–1328, 2016.

[11] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, presented at the 27th Conference on Computer Communications, INFOCOM, 2008.

[12] C. Zhang, P. H. Ho, and J. Tapolcai, On batch verification with group testing for vehicular communications, Wireless Networks, vol. 17, no. 8, pp. 1851–1865, 2011.

[13] A. Shamir, Identity-based cryptosystems and signature schemes, Lecture Notes in Computer Science, vol. 196, pp. 47–53, 2000. [12] C.-C. Lee and Y. Lai, Toward a secure batch verification with group testing for VANET, Wireless Networks, vol. 19, no. 6, pp. 1441–1449, 2013.

[14] S.-J. Horng, S.-F. Tzeng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, Enhancing security and privacy for identity-based batch verification scheme in VANET, IEEE Trans. on Vehicular Technology, 2015. doi: 10.1109/TVT.2015.2406877.

[15] P. Guo, J. Wang, B. Li, and S. Lee, A variable threshold-value authentication architecture for wireless mesh networks, Journal of Internet Technology, vol. 15, no. 6, pp. 929–936, 2014.