International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 2 – FEBRUARY 2016.

UPGRADE RELIABILITY FOR NOVEL IDENTITY-BASED BATCH VERIFICATION SCHEME IN VANET

S.Naveena devi[1], M.Mailsamy[2] and N.Malathi[3]

[1]*PG Scholar,* [2]*Assistant Professor,* [3]*Assistant Professor*
[1, 2, 3] *Dept. of Information Technology, Vivekananda College of Engineering for Women, Tiruchengode-637205*

***Abstract*--A novel Identity-based Batch Verification Scheme in Vehicular ad hoc network (VANET) can outstandingly improve the traffic safety and effectiveness. The basic idea is to allow vehicles to send traffic message to roadside units (RSUs) or other vehicles. Vehicles have to be prohibited from some attacks on their privacy and misuse of their private data. For this reason, the security and privacy protection issues are important prerequisites for VANET. The Novel identity-based batch verification scheme was newly future to make VANET more secure and efficient for practical use. The current IBV system exist some security risks. To set up an improved scheme that can satisfy the security and isolation desired by vehicles. The proposed NIBV scheme provides the verifiable security in the casual Mysql model. In addition, the batch confirmation of the proposed scheme needs only effectual approach for VSNs to achieve confirmation, reliability, and authority. However, when the number of signatures received by a Roadside Unit(RSU) becomes bulky, a scalability problem appear immediately, where theRSU could be difficult to consecutively verify each received signature within 300 ms period according to the current committed short range communications broadcast protocol. To introduce a new identity-based batch verification scheme for transportation between vehicles and RSUs, in which an RSU can confirm abundant received signatures at the same instance such that the total verification time can be drastically reduced.**

Index Terms: **Authenticity, novel batch verification, Privacy, Vehicular ad-hoc network.**

I. INTRODUCTION

VANETs are a subgroup of mobile ad-hoc networks. The main difference is that the mobile routers construction the network are vehicles like cars or trucks and their movement is controlled by factors like road route, surrounding traffic and traffic system. It is a feasible supposition that the members of VANETs can connect to fixed networks like the Internet occasionally, at least at usual service intervals. A main goal of VANETs is to enhance road safety. In VANET they have three important entities like trusted authority, road side unit, on board unit. In trusted authority (TA) schedule the route to the vehicle. The TA can communicate via a road side unit (RSU).In RSU is a communication between the TA and OBU. In OBU to commune with roadside units (RSUs) situated at roadside or street intersection. Vehicles can also use OBUs to commune with each other. VANET can be classifying into two types: vehicle-to-infrastructure (V2I) communication or inter-vehicle (V2V) communication. The basic use of VANET is that OBUs at regular intervals transmit information on their nearby states. The information like current time, position, direction, speed and traffic events are passed to other nearby vehicles and RSUs. For example, the traffic actions could be accident location, brake light warning, change lane/merge traffic warning, emergency vehicle warning, etc. Other vehicles may modify their travelling routers and RSUs may inform the traffic control centre to alter traffic lights for avoiding possible traffic jamming. VANET offers a variety of services and profit to users, and thus deserve deployment efforts. The wonderful benefits expected from vehicular communications and the enormous number of vehicles, it is clear that vehicular communications are probable to become the most relevant understanding of mobile ad hoc networks. The appropriate integration of on-board units and position devices, such as GPS receivers along with communiqué capabilities, opens marvelous business opportunities, but also raises alarming research challenges.

The protection of communication exchange acting a key task in VANET applications. The message from OBUs has to be identity-authenticated and integrity-checked before it can be trust on. Otherwise, an opponent can change the information or even masquerade as other vehicles to transmit the wrong information. The wrong information probably makes some bad situation. For example, the information of incorrect traffic flow may reason the traffic control centre to make wrong decision. The traffic light of the heavy side always stay red and the other side stay green. In addition, an opponent may portray an ambulance to require the traffic light to help with her/him and break the driving right of other users.

A driver may not wish for others to know her/his travelling routes by tracing information sent by OBU. Or else, it is hard to draw users to link the network. So, an nameless communication is needed. On the opposing, traceability is also necessary where a vehicle's real identity should be able to be exposed by a trust authority for legal responsibility issue when crimes or accidents happen. For example, a driver who sent out false information causing an accident should not be clever to escape by using a nameless identity. In other words, vehicles in VANET need the provisional privacy.

Our main aid in the paper is given as follows: Specified the security issues of avoiding incorrect information and the contradictory goals of isolation and traceability. The proposed new identity based batch verification scheme can be used in both V2I and V2V communications. The new IBV scheme can endure our future threats such as the identity privacy violation, fake and anti-traceability attacks. Compare to the preceding schemes, the future new IBV scheme is efficient in computational cost of confirmation delay. It is since the process of batch verification needs only a small stable number of pairing and point increase computations. In new identity batch verification scheme can improving the security using efficient algorithm like symmetric encryption algorithm and new identity based batch verification algorithm.

II. RELATED WORKS

In 2015, Shiang-Feng Tzeng, Shi-Jinn Horng [1] proposed a scheme to point out that the present IBV scheme survive some security risks. To introduce an improved scheme that can satisfy the security and privacy needed by vehicles. The IBV scheme provides the demonstrable security in the random oracle model. Lee and Lai [2] described the two weakness of *et al.*'s IBV scheme. First, Zhang *et al.*'s IBV system is susceptible on the replay attack. An opponent may replicate a false condition, such as traffic squash, by collect and store the vehicle messages and signatures in the matching condition. In 2013, Shi-Jinn Horng, Shiang-Feng Tzeng [3], SPECS provided software based key to satisfy the solitude requirement and gave inferior message slide and more successful rate than earlier result in the message verification phase. To find out that SPECS is vulnerable to imitation attack. SPECS have a pour such that a spiteful vehicle can force random vehicles to broadcast fake messages to other vehicles. In 2008, Zhang *et al* [4] proposed an identity-based batch verification system for V2I and V2V infrastructure in VANET. They adopt a one-time identity-based signature, which eliminate the confirmation and broadcast costs of certificate for public key. It reduces the general verification delay of a lot of message signatures. In 2007, Raya and Hubaux [5] proposed a scheme to conceal the real identities of users by nameless certificates. The conservative public key infrastructure is adopt as the security base to achieve both message verification and integrity. The main problem is that each vehicle loads a large storage capability to save a number of key pairs and the matching certificates, and incur the high cost of message verification.

III. PRELIMINARIES

A. SYSTEM MODEL

The structure model consists of four entities like trust authority, application servers, roadside units and on-board units (OBUs) install on vehicles. A two-layer vehicular network model was address in recent research .The top layer is a trusted authority and application servers. TA and application servers converse with RSUs through secure channel, the transport layer security protocol, by wired relations. The lower layer is embrace of vehicles and RSUs. The communiqué amongst them is based on the dedicated short range communications protocol. The VANET security standard, every vehicle has its own public/private key pairs distributed by TA. Before messages are transmit, vehicles contain to sign the messages with their private keys to assurance the honesty of messages. Delivery the safety related or non-traffic related message, each RSU or vehicle is accountable for verify their signatures of messages.

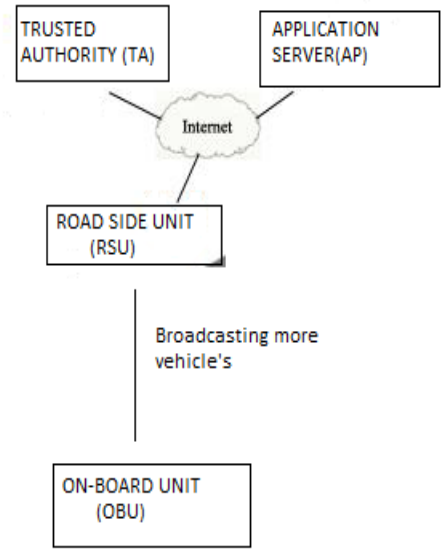

FIG 1: The System Model

1) TA is totally confidential by everybody and it is motorized with enough calculation and storage ability. The laid off TA are installing to keep away from being a bottleneck or a solitary point of failure.2) TA is the only can decide the vehicle's real individuality but not by other vehicles or RSU.
3) TA and RSUs converse via a secure fixed network.
4) RSUs are not confidential. As they are located down road side, they can be simply co-operation. They are inquisitive about vehicle's seclusion.
5) Tamper-proof devices on vehicles are supposed to be believable and its information is for no reason to been reveal. The WAVE standard, every OBU is capable with a hardware security module , which is a tamper-resistant module used to accumulate the security resources The HSM in each OBU is accountable for drama all the cryptographic process such as signing messages, keys update. It is hard for lawful OBUs to take out their private keys from their tamper-proof devices. The system has its individual clock for make accurate timestamp and is clever to sprint on its individual battery. TA, RSUs and OBUs have approximately coordinated clocks.

B.ADVERSARY MODEL

All participating RSUs and OBUs are not believable and the communication channel is not protected. An opponent is able to performing the following without the novel IBV scheme.

1) An opponent may adjust or repeat existing messages, even an opponent may disperse or mimic any rightful vehicle to produce incorrect information into the scheme to influence the behavior of other users or damage the transportation of VANET.

2) An opponent may draw the real identity of any vehicle and can disclose the vehicle's real identity by analyzing many messages sent by it.

IV. PROPOSED SYSTEM

(1)The OBU of the vehicle broadcast or distribute traffic information to RSU or nearby vehicles. (2)RSU verify the traffic information and send to the TA. (3)TA schedules the route of the vehicles, which route is traffic free and shortest. (4)To applying a dynamic routing algorithm find shortest energetic routers without traffic. (5)Energy level should be increased in vehicular networks during that time of providing high security. (6)To apply a novel identity based batch verification algorithm deducts the hacking packets and also find, which vehicle can be create it. To compromise the particular hacking vehicles master keys. (7)To apply a novel identity based batch verification scheme provide high security and high performance for vehicular networks.

(8)Compare to existing system, High Security can be provided. RSU extend network range. (9)In novel identity based batch verification scheme easily identify the changed information and difficult to access the information without signature key. (10)TA easily fined the duplicate information and provides high performance in novel IBV scheme. (11)Advanced symmetric key algorithm can be used to novel identity based batch verification. (12)Novel identity based batch verification algorithm can be used to improving a security of a VANET and also improving a speed and performance.

V. PERFORMANCE EVALUATION

The computation delay is the mainly important issue, which affect the worth of traffic linked messages. To describe the time charge of the cryptographic linked operations necessary in each signing and verification by the novel IBV scheme and other batch verification schemes.

In fig.2 is comparison between computations delay and verify a signing message. A previous IBV schemes they have more delay for verifying a message. Previous IBV scheme have a delay of 9.6 in verification and 0.6 in sign message.

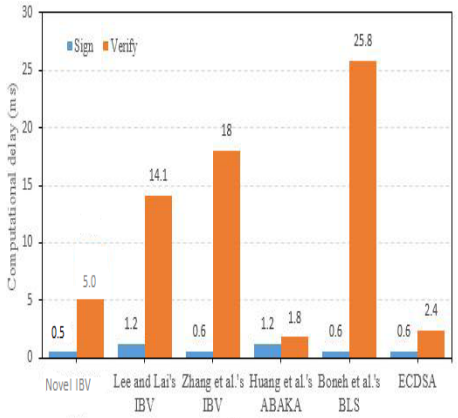

FIG 2: Comparison of computational delay to verify and signing message

To proposed a novel IBV scheme having a 5.0 in verification delay and 0.5 in signing a message.

Fig. 3 indicates the connection between the transmission overhead and the number of messages received by an RSU in 10 seconds. As the number of messages increases, the transmission overhead increases linearly. The transmission overhead of the novel IBV system

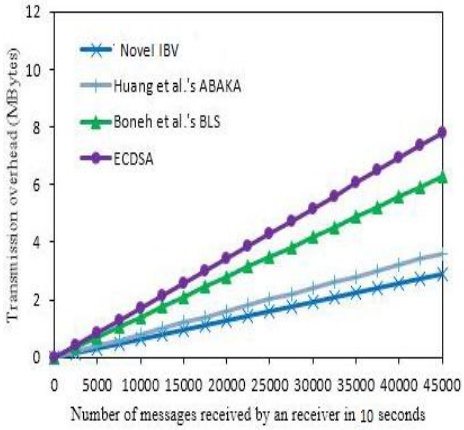

FIG 3: Transmission overhead with number of message received

is least among the four schemes. Here, 45,000 correspond to the number of messages transmitted by 150 vehicles in 10 seconds. The previous IBV systems they have transmitted by 150 vehicles in 30 seconds.

VI. CONCLUSION

To proposed an efficient identity-based batch verification (NIBV) scheme for vehicle-to-infrastructure and inter-vehicle communications in vehicular ad hoc network (VANET). The batch-based verification for multiple message signatures is more efficient than one-by-one single verification when the receiver has to confirm a large number of messages In particular; the batch verification process of the proposed NIBV scheme needs only a constant number of pairing and point multiplication computations, independent of the number of message signatures. The proposed NIBV scheme is secure against existential forgery in the random oracle model under the computational Diffie-Hellman problem. In the performance analysis, we have evaluated the proposed NIBV scheme with other batch verification schemes in terms of computation delay and transmission

overhead. Moreover, we verify the efficiency and practicality of the proposed scheme by the simulation analysis. Simulation results show that both the average message delay and message loss rate of the proposed IBV scheme are less than those of the existing schemes.

VII. FUTURE WORK

In the future work, we will continue our efforts to enhance the features of IBV scheme for VANET, such as recognizing illegal signatures. When attackers send some invalid messages, the batch verification may lose its efficacy. This problem commonly accompanies other batch-based verification schemes. Therefore, thwarting the invalid signature problem is a challenging and a topic for study in our future research.

REFERENCE

[1] Shiang-Feng Tzeng, Shi-Jinn Horng,
"Enhancing security and privacy scheme for identity based batch verification scheme in VANET," IEEE Transaction on Vehicular technology, 2015.
[2]C. C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for VANET," Wireless Networks, vol. 19, no. 6, pp. 1441-1449, 2013.
[3]Shi-Jinn Horng, Shiang-Feng Tzeng, "b-SPECS+: Batch Verification for Secure
Pseudonymous Authentication in VANET", information forensics and security, vol. 8, no. 11, November 2013.
[4]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 the 27th IEEE International Conference on Computer Communications (INFOCOM'08), pp. 816-824, 2008.
[5] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security – Special Issue Security Ad Hoc Sensor Networks, vol. 15, no. 1, pp. 39-68, 2007.