Weighted Priority Based Signatures' Batch Verification Scheme in Vehicular Ad-Hoc Networks

Zeeshan Shafi Khan, Abdullah Alaraj, S. Nithya Rekha, Farzana Azam, Muhammad Zubair

Abstract: **In order to improve performance and to reduce the delays, batch verification of signatures in Vehicular Ad-hoc Networks (VANETs) has been used by many researchers. Later on, Absolute priority was introduced along with the batch verification of signatures. This paper presents a new weighted priority based signature's verification scheme that not only increases the efficiency of batch verification but also results in mitigating the starvation issues. The proposed scheme is evaluated and results are presented in order to show the validity and contribution of the scheme.**

Index Terms: **Signatures' Batch Verification, Weighted Priority, Vehicular Ad-hoc Networks**

I. INTRODUCTION

In Vehicular Ad-hoc Networks (VANETs), vehicles are equipped with On-board Units (OBUs) which allow the travelers to share valuable information. There are two types of communications in VANETs, namely, Vehicle-to-Vehicle (V2V) communication where OBU communicates with another OBU, and Vehicle-to-Infrastructure (V2I) communication where OBU communicates with Road Side Unit (RSU) located at the roadside. The communication uses dedicated short range communications (DSRC) protocol. Each vehicle periodically broadcasts messages about its conditions and road conditions. The broadcasted messages will help other drivers of vehicles to drive safely and avoid traffic problems like accidents, weather conditions, congestions, etc. The structure of VANETs is composed of two layers, namely, the upper layer and the lower layer. The application servers reside in the upper layer. Road side units (RSUs) and vehicles (OBUs) reside in the lower layer. The nature of VANETs makes them vulnerable to attacks. Therefore, it is very important to secure the VANETs environment because some of its applications are safety-related. Attackers can modify, delete, replay messages transmitted in VANETs [1].

Paper submitted August 18, 2016, revised December 16, 2016.

The authors are with College of Computer, Qassim Private Colleges, Saudi Arabia, Department of Information Technology, Qassim University, Saudi Arabia

Zeeshan Shafi Khan, zeeshanshafikhan@gmail.com
Abdullah Alaraj, alaraj@outlook.com
S. Nithya Rekha, rekhasiva24@gmail.com
Farazana Azam, farzanaazamkhan@gmail.com
Muhmmad Zubair, zubairnet@yahoo.com

There are two types of security threats to VANETs. The first type is data threat where the VANETs information is threatened. Examples of data threats include confidentiality, integrity, availability, authenticity, and non-repudiation. The second type is the threats to VANET system that include threats to system hardware, software and system users. It is very important for a VANET system to use digital signatures to verify the messages sent between nodes. However, verifying each and every message will make the verification time too long especially in high density roads. Therefore, instead of verifying each message, vehicles and RSUs verify messages in batches [2].

II. RELATED WORK

Zhang et al. introduced an efficient batch signature verification scheme for communications between vehicles and RSUs (V2I) communications, in which an RSU can verify multiple received signatures at the same time such that the total verification time can be dramatically reduced [3]. In a situation of high traffic density a vehicle cannot verify all signatures of the messages sent by its neighbors in a timely manner, which results in message loss or significant delay. To deal with these issues Zhang et al. [4] introduced a novel RSU-aided messages authentication scheme, called RAISE. T. W. Chim et al. introduced a new signatures batch verification, SPECS, based on bloom filters to broadcast the results. The scheme produced very efficient results and is considered as one of the good batch verification solution. Re-batching is also discussed by the author [5]. Wasef et al. proposed batch verification scheme that remarkably increases the number of signatures that can be simultaneously verified. Hence, OBUs can meet the real life verification requirements of VANETs. The conducted simulation shows that the proposed batch verification scheme has the lowest message loss ratio compared to its counterparts [6].

Huang et al. introduced an anonymous batch authenticated and key agreement (ABAKA) scheme to authenticate multiple requests sent from different vehicles and establish different session keys for different vehicles at the same time [7]. Islam et al. presented an extremely efficient batch verification system from a IBGS group signature scheme for VANET environments. They have further presented a batch scheduling algorithm to accelerate batch verification. This scheme not only provides the desired level of security requirements, but also is efficient in storage and computation[8]. Horng et al. provided a secure scheme that can achieve the security and privacy requirements, and overcome the weaknesses of

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

SPECS [5]. Moreover, the authors show the merits of their scheme through performance evaluations in terms of verification delay and transmission overhead [9]. Tzeng et al. pointed out that in the current IBV scheme there exists some security risks. So they have introduced an improved scheme that can satisfy the security and privacy desired by vehicles. The proposed IBV scheme provides the provable security in the random oracle model [10]. Shao et al. proposed an efficient threshold anonymous authentication protocol for VANETs by using a new group signature scheme. The proposed threshold anonymous authentication protocol is characterized by integrating the decentralized group model and threshold authentication method to obtain threshold authentication, efficient revocation, enforceability, anonymity, and traceability for VANETs [11].

III. ISSUES IN USING PRIORITY IN BATCH VERIFICATION OF SIGNATURES

Priority is used inside VANET by many researchers. Some used priority in scheduling of messages at the time of heavy load on network [12-14]. Jinila et al. discussed priority and batch verification. But the author stated that since the batch verification scheme is subject to false signatures attack, it is better to use priority based signature verification but not in batch [15]. Kumar et al. [16] used priority for batch verification of signatures. The idea of the paper is to provide high priority to emergency vehicles therefore vehicles are divided into two priority groups by allocating high priority to emergency vehicles. Other than vehicle type, no parameter is used to assign priority to vehicle. Biswas et al. [17] assigned the priority to messages from receiver point of view. The authors used the complete priority and stated that in high traffic duration only the high priority messages can be verified by totally ignoring the low priority messages. This can results in starvation.

A lot of work has been done on batch verification of signatures in VANET but a very little attention has been given to priority based batch verification. Researchers who used priority based batch verification either assigned priority by taking vehicle type as parameter or by taking message type as parameter. According to our findings, the parameters like trust value, vehicle position, network density etc. have not been used in assigning priority to vehicle or message. As a result of this, efficiency and performance cannot be achieved as well starvation may also happen for few vehicles. Moreover, the present priority based batch verification solutions use the absolute priority scheme in order to create batch of signatures which results in starvation at the end of few vehicles. In batch verification of signatures the major challenge is that if a single signature in a batch is invalid, the whole batch will be declared invalid. In case of an invalid batch, it needs to be re-batched. Use of priority in re-batch is also one of the contribution of this paper.

IV. WEIGHTED PRIORITY BASED BATCH VERIFICATION SCHEME

This paper presents a new signature's batch verification scheme by using priority in weighted manner. To calculate priority, multiple network parameters are considered. To formulate a batch instead of using absolute priority, a weighted priority methods is employed. Moreover a mechanism for re-batching is also developed and described in the paper.

A. Priority Allocation

To assign priority to a message different network and vehicle related parameters are used in order to obtain a value that can be used in multiple scenarios. First parameter used, is the vehicle type (denoted by V). Here, type means the purpose of the vehicle like emergency vehicle, traffic authority vehicles, normal public vehicles etc. Priority of emergency vehicles is high, priority of traffic authority vehicles is medium and normal public vehicle's priority is low.

The next parameter that is used to allocate priority is the trust value of the vehicle (denoted by T). In the start when a vehicle becomes a part of the network, a zero trust value is assigned to the vehicle. As soon as vehicle starts sending and relaying the messages trust value starts to increase or decrease depending upon the actions of that vehicle. Different trust models have been studied [18] in order to select an appropriate trust model to use. After a deep analysis a trust model similar to one proposed by Wei et. al. [19] is preferred to use. So by using the trust model a trust value for each vehicle is calculated and used as one parameter to assign priority to the vehicle.

Vehicle's current position and speed (denoted by S) in the network and network density (denoted by D) are the other two parameters used to assign priority to the vehicle. In Urban areas, priority value of a vehicle is different from that of highways. Message type (denoted by M) is another parameter used to assign priority to the message. In this paper messages are classified only into two types, real time messages and non real time messages. Real time messages have higher priority over non real time messages. Since other four parameters discussed above are not subject to change with each message, so the message type is separated from these four parameters. As we are considering only two types, we assign a default priority value to each type and whenever RSU receives a message that priority value is added accordingly with the combined priority value of other four parameters. Previous priority value (denoted by PP) is also used (if any) in assigning a new priority value to the message. Priority of vehicle is updated either after a specific periodic period of time or on occurring of some special events. The special events used are leaving or joining highway, identification of malicious signature etc.

Equation (1) shows the calculation of priority for the first time. Θ stands for a function. In equation 1 it is shown that all the parameters have the same weight while calculating the priority for the first time. w represents the weight and for the first time values of w_1 to w_5 will be same.

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$P(t) = \Theta(V, T, S, D, M) \qquad \text{eq. (1)}$$

$$= [(w_1.V + w_2.T + w_3.S + w_4.D) + w_5.M]$$

In equation 2, the priority is updated, in case when a vehicle join or leave the network. When a vehicle will join or leave the highway, the two important parameters which will be changed are speed and density. Therefore in that case speed and density will have double weight as compared to other parameters. Hence the value of w_3 and w_4 will increase. The Previous priority will also be used to calculate new priority where $0 < \alpha < 1$.

$$P(t + 1) = (\alpha)\, P(t) + (1- \alpha)\, \Theta \qquad \text{eq. (2)}$$

The priority is updated in case when the signature from a vehicle is found malicious. In this case, the trust value decreases significantly and this can assume negative value. To make it even more secure, the weight of trust value is increased four times in calculating the new priority. Therefore value of w_2 will change.

B. Batch Formulation

To formulate the batch again weighted priority technique is used. By using absolute priority, there are chances of starvation for low priority vehicles. Therefore a weighted technique is used in which to formulate a batch, messages from vehicles of all priorities will be taken but however the number of messages taken from each vehicle's priority will be different depending on the weight assigned to each priority. Vehicles with high priority will have more weight as compared to vehicles of low priority. The main idea behind this solution is to improve the signature's batch verification process as well as to eliminating the starvation that often came with priority based solutions.

Messages taken from each type of priority can be calculated by using equation 3.

$$M = \frac{P_x}{\sum(P_1, P_2, \ldots\ldots..P_n)} * B \qquad \text{eq. (3)}$$

Where M is the number of messages selected, P_x is the priority of the message, and P_1 to P_n is the sum of all the other priorities. B is the size of the batch.

C. Re-Batch Process

If a signature is found malicious the whole batch will be declared invalid. In that case re-batching will be performed. There is a high probability that the malicious signature will be in one of the low priority messages. Therefore in order to avoid the malicious signature along with high priority messages, re-batching will be performed in such a way that the batch is divided into two equal parts. Priority of messages, those already have high priority, is doubled while there is no change in case of low priority messages. While re-batching, more high priority messages will be included as compared to low priority messages so that there are more chances of success in batch verification. The scenario is explained in equation 4. P_l is for messages with low priority while P_h is for messages of high priority.

$$M = \frac{P_l}{\sum(P_1, P_2, \ldots\ldots..P_n)} * B \qquad \text{eq. (4)}$$

where $P_l = P_x/2$

or

$$M = \frac{P_h}{\sum(P_1, P_2, \ldots\ldots..P_n)} * B \qquad \text{eq. (5)}$$

where $P_h = P_x * 2$

V. TESTING, RESULTS AND DISCUSSION

We conducted various experiments in order to evaluate the efficiency of our solution. We divided our experiments into two sets. In the first set we measure the efficiency and accuracy in batch verification while in the second set of experiments it is investigated that whether the solution mitigate the starvation issues or not. For simulation we created a setup of 200 vehicles where every vehicle randomly sends 1 to 10 messages in one minute. Simulation is run for 60 minutes. At time of joining a priority value is assigned to the vehicle by considering its type, density and speed and at the time of update trust and previous priority is also used. In normal scenario priority is recalculated periodically after every 10 minutes. Maximum batch size is fixed at 50. Vehicles are divided into two types, legitimate and malicious and it is defined at the start of the experiment. Value of α is taken as 0.1.

A. Experiment 1: Average Rounds to Verify High Priority Messages

The first set of experiments is conducted to calculate the average round consumed to verify the high priority messages in the presence of different number of attackers. Vehicle's priority values are in the range of -3 to +3 where positive values are considered as high priority. Figure 1 explains the results of this set of experiments. In figure 1, on the x-axis we have the number of rounds those are performed by the RSU to validate the signatures of high priority vehicles. As shown on the y-axis of figure 1, the experiments are conducted by taking different percentage of malicious vehicles. It is investigated that how many extra rounds are needed when number of malicious vehicles increases in the network.

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

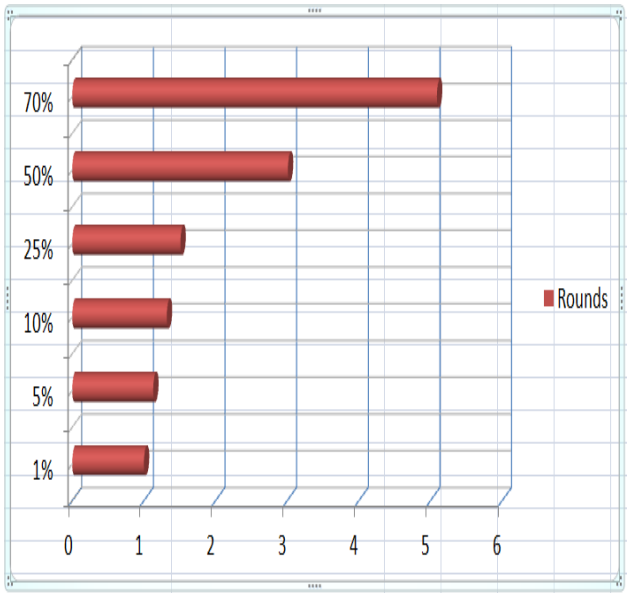

Fig. 1: Average Rounds to Verify High Priority Messages

B. Experiment 2: Verification of High Priority Messages in first second and third round of batch verification

In the second set of experiments the percentage of high priority messages which are verified in first, second and third round of batch verification is calculated. As done in the previous experiment, positive values are considered as high priority values. In figure 2 y-axis represents the percentage of high priority messages which are verified while the x-axis consists of various percentages of malicious vehicles. When number of malicious vehicles increases in the network percentage of messages verified in each round decreases accordingly. Results are explained in figure 2.

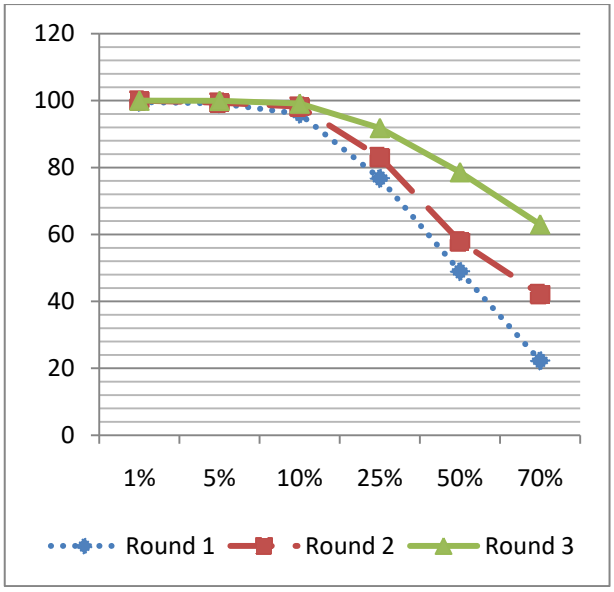

Fig. 2: Verification of High Priority Messages in first, second and third round of batch verification

C. Experiment 3: Batch Formulation and Inclusion of Messages from Different Priorities

As it is claimed in this paper that the proposed scheme discourages the starvation so to prove this claim, the third set of experiments is conducted. Seven different priority values are assigned to all the vehicles in the network. After that it is investigated that when forming a batch how many messages are taken from vehicles of each priority. Whether the low priority vehicles are totally ignored or starvation is minimized is explained in figure 3. Y-axis of figure 3 represents the percentage of messages taken from each priority value while x-axis represents the priority values.

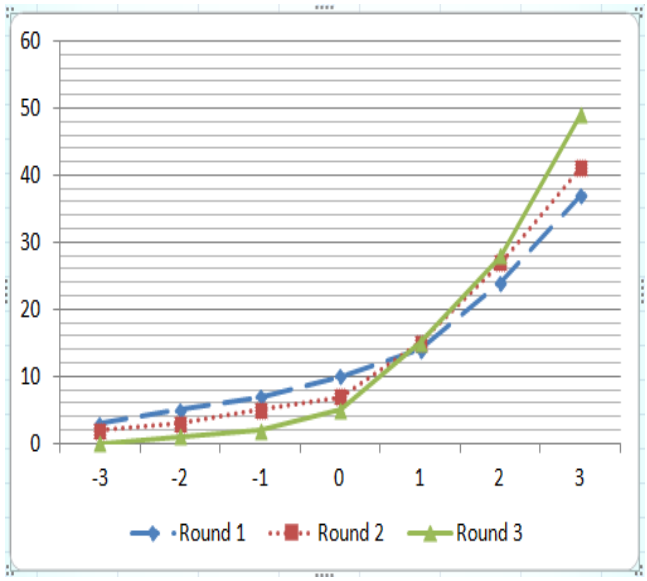

Fig. 3:Share of Each Priority in Batch Formulation

VI. CONCLUSION

In this paper a new weighted priority based technique for batch verification of signatures in VANETs is developed. In this scheme, the priority is allocated to the messages by considering number of vehicle's and network's parameters. To formulate a batch of signatures weights are used and each priority has its share in the batch. This mechanism results in reducing the mitigating issues in priority based batch verification. To obtain more efficiency in case of invalid batch a re-batching solution is also provided that tries to separate the possible malicious signature based message from the other high priority messages.

REFERENCES

[1] Mohammed Saeed Al-kahtani, " Survey on security attacks in Vehicular Ad hoc Networks (VANETs)", 6th International Conference on Signal Processing and Communication Systems (ICSPCS), QLD, 2012, pp. 1 - 9

[2] Vinh Hoa LA, Ana CAVALLI, " Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey", International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014

[3] C. Zhang, X. Lin, R. Lu, P.H. Ho, and Xuemin Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Networks", in the proceedings of the IEEE INFOCOM 2008, pp. 816-824.
[4] C. Zhang, X. Lin, R. Lu, P.H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks", in the Proceedings of the IEEE ICC, May 2008, pp. 1451–1457.
[5] T.W. Chim a, S.M. Yiu a, Lucas C.K. Huia, Victor O.K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs", Ad Hoc Networks, vol. 9, no. 2, 2011, pp. 189-203.
[6] Albert Wasef and Xuemin Shen, "Efficient Group Signature Scheme Supporting Batch Verification for Securing Vehicular Networks", in the proceedings of the IEEE ICC 2010, pp. 1-5.
[7] Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks", in IEEE Transactions on Vehicular Technology, Vol. 60, No.1, January 2011, pp.248-262.
[8] Mohammad Saiful Islam Mamun and Atsuko Miyaji , "An Optimized Signature Verification System for Vehicle Ad hoc NETwork", in the 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2012.
[9] Shi-Jinn Horng, Shiang-Feng Tzeng, Yi Pan, Pingzhi Fan, Xian Wang, "b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET", published in IEEE Transactions on Information Forensics and Security , Vol.8 , Issue 8, 2013, pp. 1860 – 1875.
[10] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhmmad Khurram Khan, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET", in the IEEE Transactions on Vehicular Technology, Volume: PP , Issue: 99, 2015.
[11] Jun Shao, Xiaodong Lin, Rongxing Lu, and Cong Zuo, "A Threshold Anonymous Authentication Protocol for VANETs", in the IEEE Transactions on Vehicular Technology, Vol.65, Issue: 3, 2015, pp. 1711 – 1720.
[12] Parixit Patel, Dhaval Varia, "Priority Based Scheduling by Achieve Better Service Ratio in VANET", IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 01, 2014
[13] Abubakar Aminu Mu'azu, Low Jung Tang, Halabi Hasbullah, Ibrahim A. Lawal, Peer Azmat Shah, "Real-Time Massage Differentiation with Priority Data Service Flows in VANET", 2014 International Conference on Computer and Information Sciences (ICCOINS), p. 1-6, Malaysia, 3-5 June 2014
[14] Tripti C, Jibu Kumar M.Gy and Manoj R, " Priority based Control Channel Access Scheme for Throughput Improvement in VANET", 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015
[15] Y. Bevish Jinila, K. Komathy, IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013), p. 456-46, Chennai, 12-14 Dec. 2013
[16] P. Vinoth Kumar, M. Maheshwari, " Prevention of Sybil attack and priority batch verification in VANETs", 2014 International Conference on Information Communication and Embedded Systems (ICICES), p. 1-5, Chennai, 27-28 Feb. 2014
[17] Subir Biswas, Jelena Mi˘si´c, "Relevance-based Verification of VANET Safety Messages", IEEE ICC 2012 - Wireless Networks Symposium, 2012
[18] Bata Krishna Tripathy, Padmalochan Bera, Mohammad Ashiqur Rahman, " Analysis of Trust Models in Mobile Ad Hoc Networks: A Simulation Based Study", 2016 8th International Conference on Communication Systems and Networks (COMSNETS), 2016
[19] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning", IEEE Transactions On Vehicular Technology, Vol. 63, No. 9, pages 4647-4658, November 2014.

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)