International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 8 Issue 1 –APRIL 2014.

# Securable Message Authentication System in Vehicular Ad Hoc Networks by using Trusted Authority

Ranjitha. P
Final Year M.Tech CSE,
Vedavyasa Institute of Technology,Calicut

***Abstract*— The number of automobiles has been increased on the road in the past few years. Due to high density of vehicles, the potential threats and road accident is increasing. Wireless technology is aiming to equip technology in vehicles to reduce these factors by sending messages to each other. VANETs have emerged as a promising approach to increasing road safety and efficiency. This can be accomplished in a variety of applications that involve communication between vehicles, such as warning other vehicles about emergency braking etc. Message authentication is a common tool for ensuring information reliability, namely, data integrity and authenticity. When the number of messages that are received by a vehicle becomes large, traditional authentication may generate unaffordable computational overhead on the vehicle and therefore bring unacceptable delay to time-critical applications. An efficient cooperative authentication scheme for VANETs is adopted. To reduce the authentication overhead on individual vehicles and shorten the authentication delay, the scheme maximally eliminates redundant authentication efforts on the same message by different vehicles. To resist various attacks, and encourage cooperation, the scheme uses an evidence-token approach to control the authentication workload, without the direct involvement of a trusted authority (TA). When a vehicle passes a roadside unit (RSU), the vehicle obtains an evidence token from the TA via the RSU. This token reflects the contribution that the vehicle has made to cooperative authentication in the past, which enables the vehicle to proportionally benefit from other vehicle's authentication efforts in the future and thus reduce its own workload. To reduce the TA overload, a novel approach namely Buddy List Approach is proposed as the future work. The Buddy List approach avoids TA to the maximum and message authentication is done by each vehicles participating in the network. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.**

**Keywords- Cooperative authentication, free-riding attacks, Selfishness, vehicular ad hoc networks (VANETs)**

## I. INTRODUCTION

VANETs are subgroup of Mobile Ad hoc Networks (MANETs) with the distinguishing property that the nodes are vehicles like cars, trucks, buses and motorcycles. The primary VANETs goal is to increase road safety. To achieve this, the vehicles act as sensors and exchange warnings. A VANET uses moving cars as nodes in a network to create a transportation network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. In VANET, rather than moving at random, vehicles tend to move in an organized fashion. Each individual vehicle participates in a cooperative environment for message authentication. A central TA provides registration to vehicle users during which vehicles pseudonyms and secrets are updated and stored in the vehicles OBU. The security is more crucial in VANET due to involvement of critical life threatening situations. Some of the security issues are in handling malicious/misbehaving as well as faulty nodes. The attackers may be insider, outsider, malicious or rational. Handling message attacks includes bogus information, false positioning, privacy (disclosure of ID), denial of service and masquerading. Communication is mainly performed based on exchange of messages. Security largely depends on trust worthiness of messages that are exchanged between the nodes. On the other hand, security in VANET can be established by valid communication between trusted vehicles/nodes.

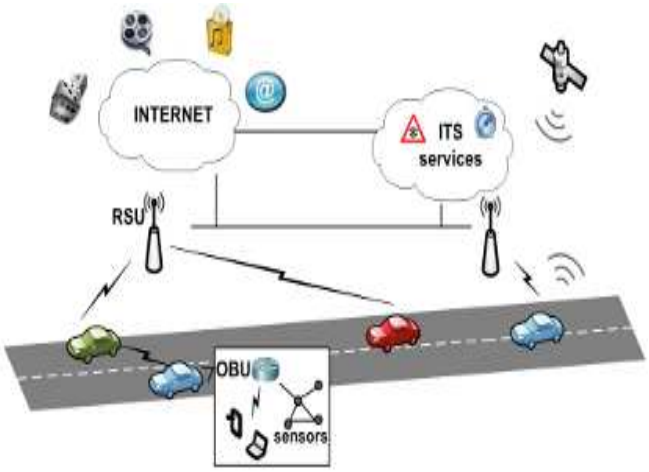


Figure 1 Secure Message Authentication Processes

Message authentication is a security measure in which the sender of the message is verified for every message sent. Message authentication is considered as one of the major security problem in VANET. Message authentication allows one party say the sender to send a message to another party say the receiver in such a way that if the message is modified in route, then the receiver will almost certainly detect this. Message authentication is also called data-origin authentication. Message authentication is said to protect the integrity of a message, ensuring that each message that it is received and deemed acceptable is arriving in the same condition that it was sent out with no bits inserted, missing, or modified. Achieving message authentication consists of two essential security checks, i.e., an integrity check and identification check. Message authentication must be implemented to allow vehicle users to differentiate reliable information. A solution to this problem in VANETs is to digitally sign messages before sending them; not only does this allow the receiver to identify the sender, but the signature also prevents the message contents from being modified. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

The rest of the paper will be organised as follows: In section 2, we see about the related works of the paper. In section 3, we discuss about the proposed method. The algorithms and simulation are shown in the section 4 and 5. The conclusion of our paper is in section 6.

## II. Related Works

In this section, we will see some of the related works to using different approaches:

In the year 2007, G. Calandriello, P. Papadimitratos, J.-P. Hubaux and A. Lioy have proposed effective and robust operations [1] that are critical for the deployment of VANETs. Mechanisms that reduce the security overhead for safety beaconing, and retain robustness for transportation safeties were designed. Moreover, to enhance the availability and usability of privacy-enhancing VANET mechanisms, the proposal enables vehicle on-board units to generate their own pseudonyms, without affecting the system security. Generally, Message authentication, integrity, and non-repudiation, as well as protection of private user information are identified as primary requirements. Pseudonymity or pseudonymous authentication requires that each node is equipped with multiple credentials, termed as pseudonyms. Thus, messages signed under different pseudonyms cannot be linked. VANET is mentioned as an application for group signatures, that is, cryptographic primitives for anonymous authentication. This is a stronger property than pseudonymous authentication, as any two group signatures generated by a node cannot be linked. Pseudonymous authentication has already gained wide acceptance in the VANET, while anonymous authentication incurs additional overhead. This led them to focus on pseudonym-based systems.

X. Lin, X. Sun, P.-H. Ho, and X. Shen, has presented a secure and privacy-preserving protocol for vehicular communications called Group Signature and Identity (ID)-based Signature (GSIS) [2]. According to them, security problems are divided into two fold: Security and Privacy Preservation between the OBUs and OBUs and between the OBUs and the RSUs. Group signature was used to secure the communication between the OBUs and OBUs, whereas, a signature scheme using ID-based cryptography (IBC) was adopted in the RSUs to digitally sign each message launched by the RSU to ensure its authenticity. With group signature, security, privacy and efficient traceability can be achieved. On the other hand, the management complexity on the public key and the certificate can be reduced with the ID- based signature. To enhance the performance and to reduce the communication overhead, an efficient broadcast authentication protocol called TESLA (Timed Efficient Stream Loss- Tolerant Authentication) has proposed.

The concept of AEMA [3] was described by Haojin Zhu in the year 2008. The concept of AEMA was to achieve efficient authentication on emergency events in VANETs. This mainly incurs to validate an emergency event. For reducing the transmission cost, the author made use of syntactic aggregation and cryptographic aggregation technique. According to Haojin Zhu, “During the emergency messages opportunistic data forwarding process, a vehicle can hold multiple message which can be aggregated into a single one before the vehicle launches aggregated message in the air”.

This paper adopts a batch verification technique for efficient emergency message verification to reduce the computation cost. The fast propagation of emergency and local warning messages to the approaching vehicles will be helpful for preventing secondary accidents. In most cases, a VANET carries out such emergency message propagation in a multihop transmission manner, particularly in the suburban areas where less RSU are installed. In particular, there launched a voting mechanism in which crosschecking the emergency event by collecting the feedback of witnesses was defined which was originally used to detect the misbehaving nodes in a distributed ad hoc network without any centralized security authority. The mechanism can be migrated to VANETs to enhance the overall security of emergency events authentication. A voting scheme was implemented on location based groups, where vehicles are grouped according to their location. According to the author, the voting mechanism effectively improves the security of VANET at the expense of increased computation and transmission overhead.

Vehicular Sensor Networks (VSNs) [4] focus on the human driving experiences and traffic flow control systems. C. Zhang, R. Lu, X. Lin, P.-H. Ho and X. Shen employed a digital signature scheme that 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. An efficient batch signature verification scheme for communications between vehicles and RSUs (or termed vehicle- to-Infrastructure (V2I) communications) was adopted, in which an RSU can verify multiple received signatures at the same time such that the total verification time can be reduced.

A novel RSU- aided message authentication scheme [5] was presented in the year 2008 by C. Zhang to reduce the communication overhead imposed by the previous paper. When the traffic density becomes larger, a vehicle cannot verify all signatures of the messages sent by its neighbours in a timely manner, which results in message loss. A novel RSU-aided messages authentication scheme, called RAISE was introduced. With RAISE, roadside units (RSUs) are responsible for verifying the authenticity of the messages sent from vehicles and for notifying the results back to vehicles. In VANETs, vehicles are equipped with wireless on-broad units (OBUs), which communicate with each other or with roadside units (RSUs) with a dedicated short range communications (DSRC) protocol. According to DSRC, each vehicle periodically broadcast its routine traffic-related information containing its current speed, location, deceleration/acceleration, etc. With the received information, other drivers can make an early response in case of exceptional situations such as accidents, emergent braking, and traffic jams. RAISE explores the unique features of VANETs by employing RSUs to assist vehicles in authenticating messages. Each IVC message will be attached with a short keyed hash message authentication (HMAC) code generated by the vehicle, and the corresponding RSU in the range will verify these HMACs and disseminate the notice of authenticity to each vehicle. Compared to the previous paper, with the implementation of RAISE, communication overhead is reduced and deals with scalability issue too. With the key chain commitments distributed by RSUs, a vehicle can effectively authenticate any received message from vehicles nearby even in the presence of frequent group membership fluctuation. Compared with previously reported public key infrastructure (PKI)- based packet authentication protocols for security and privacy, the communication overhead and computation cost of the proposed protocol are significantly reduced due to the adoption of a short message authentication code (MAC) tag attached in each packet for the packet source authentication and packet integrity check.

C. Zhang has described a novel roadside unit (RSU)-aided message authentication scheme [6] named RAISE. In the case of the absence of an RSU, a supplementary scheme has been proposed, where vehicles would cooperatively work to probabilistically verify only a small percentage of these message signatures based on their own computing capacity. Each safety message will be attached to a short message authentication code (MAC) generated by the sender under the secret key shared between the sender and an RSU. The RSU helps to verify MACs. RAISE improves the authentication efficiency and reduces the communication overhead in the mean time. In a case where the presence of RSUs is not pervasive at the beginning of the VANET deployment stage, a supplementary scheme, i.e., cooperative message authentication scheme (named COMET) was used, which works in the absence of RSUs. With COMET, vehicles do not need to verify all the message signatures that they receive from their neighbouring vehicles; instead, they cooperatively work and verify a small percentage of these message signatures with some probability based on their own computing capacity. As such, the authentication efficiency can be improved, and a low message loss ratio (LR) can also be guaranteed compared to the previous work.

Y. Hao, Y. Cheng, C. Zhou, and W. Song have proposed a study that mentioned a distributed key management framework [7] based on group signature to provision privacy in vehicular ad hoc networks (VANETs). Each road side unit (RSU) acts as the key distributor for the group. It addresses the issue of large computation overhead due to the group signature implementation. A practical cooperative message authentication protocol has thus proposed to reduce the

verification burden, where each vehicle only needs to verify a small amount of messages. The centralized key management has some disadvantages. For instance, the system maintenance was not flexible. Another issue regarding the centralized key management was that many existing schemes assume a tamper-proof device being installed in each vehicle. In a secure distributed key management framework, the road side units (RSUs) were responsible for secure group private keys distribution in a localized manner. When a vehicle approaches an RSU, it gets the group private key from the RSU dynamically. All vehicles which get the group private key from the same RSU form a group. A compromised RSU may deliver other vehicles group private keys.

Receiver-location privacy is an important security requirement in privacy-preserving Vehicular Ad hoc Networks (VANETs). An efficient social-tier-assisted packet forwarding protocol, called STAP [8] has introduced by X. Lin, R. Lu, X. Liang, and X. Shen, for achieving receiver-location privacy preservation in VANETs. Vehicles often visit some social spots, such as well-traversed shopping malls and busy intersections in a city environment, deploy storage-rich Roadside Units (RSUs) at social spots and form a virtual social tier with them. Then, without knowing the receiver's exact location information, a packet can be first forwarded and disseminated in the social tier. Later, once the receiver visits one of social spots, it can successfully receive the packet. The STAP protocol can protect the receiver's location privacy against an active global adversary, and achieve vehicle's conditional privacy preservation as well. A social-tier-assisted packet forwarding protocol (STAP) for VANET mainly make use of the people's lifestyle and the characteristics of social tier in VANETs to improve the packet delivery performance, and achieve the receiver-location privacy preservation.

In this paper, Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang and Xuemin Shen have proposed an effective pseudonym changing at social spots (PCS) strategy [9] for location privacy in VANETs. Frequent pseudonym changing provides a promising solution for location privacy in VANETs. If the pseudonyms are changed in an improper time or location, such a solution may become invalid. To deal with this issue, in this paper, they present an effective pseudonym changing at social spots (PCS) strategy to achieve the provable location privacy. Specifically, they introduced the social spots where many vehicles may gather that better location privacy can be achieved when a vehicle changes its pseudonyms at some highly social spots, and the proposed PCS strategy can assist vehicles to intelligently change their pseudonyms at the right moment and place. To achieve location privacy, a popular approach recommended in VANETs is that vehicles periodically change their pseudonyms when they are broadcasting safety messages. A vehicle must hold a certain amount of pseudonyms. A simple solution was proposed, where an OBU device equipped on a vehicle possesses a large number of anonymous short-time keys authorized by a Trusted Authority (TA). Obviously, the solution can achieve conditional location privacy when periodically changing the pseudonyms. However, it may take a large storage space to store these short-time keys in OBU device. GSIS is a group signature based technique which can achieve conditional location privacy without pseudonyms changing. However, the pure group signature verification is usually time-consuming which may be not suitable for some time-stringent VANET applications. ECPP is another anonymous authentication technique which combines group signature and ordinary signature. In ECPP, when a legal vehicle passes by an RSU, the RSU will authorize a group signature based short-life anonymous certificate to the vehicle. Once receiving a signed message, anyone can verify the authenticity of message by checking both the anonymous certificate and message signature. When the vehicle signs many messages, any verifier only needs execute one group signature verification operation on certificate, thus it is more efficient than GSIS. Similar to ECPP, Calandriello et al., inspired by the idea of pseudonymous PKI for ubiquitous computing, also combine group signature and ordinary signature techniques to achieve anonymous authentication in VANETs.

## III. PROPOSED WORK

In the existing work, all vehicles believed on Trusted Authority (TA) which leads to the need of a centralized authority for controlling the overall network. It is infeasible for any attacker to compromise. Thus, creates a burden to message authentication scheme and overload to Trusted Authority. Attacks by compromised vehicles or outside adversaries and only focus on user selfish behavior in cooperative authentication are not considered. Since cooperative authentication is conducted in an unattended and autonomous environment, vehicles may selfishly behave to take advantages of others authentication effort and does not exploit their own effort. Such selfish behavior, which is referred to as a free-riding attack, poses a serious threat to cooperative message authentication. On the one hand, cooperative behavior can largely reduce authentication overhead for every vehicle. Since VANETs are highly dynamic environments and the privacy of vehicles needs to be guaranteed by pseudonyms, the cooperation among vehicles can be regarded as a non repeated game where defection is always the optimal strategy for individual vehicles. To overcome the incentive to defect, we introduce an evidence-token mechanism and an ID-Based Signcryption (IBSC) scheme. We then propose a secure cooperative authentication scheme, which provides an efficient and secure cooperation platform for vehicles. The basic principal of the evidence-token mechanism is to balance the effort that vehicles make

over time with the advantages that vehicles take from others. The mechanism requires time to be slotted. The TA will be responsible for maintaining the balance according to the time slots. It receives the evidences from vehicles via RSUs when vehicles pass by the RSUs, and it sends the tokens back to the vehicles based on the evaluation of their authentication efforts in the past time slots. The evidences will not be repeatedly used to count their effort. The TA generates and distributes tokens to vehicles to enable them to verify other vehicles integrated signatures. The tokens must be of timeliness; otherwise, vehicles may disconnect from RSUs after obtaining enough tokens.

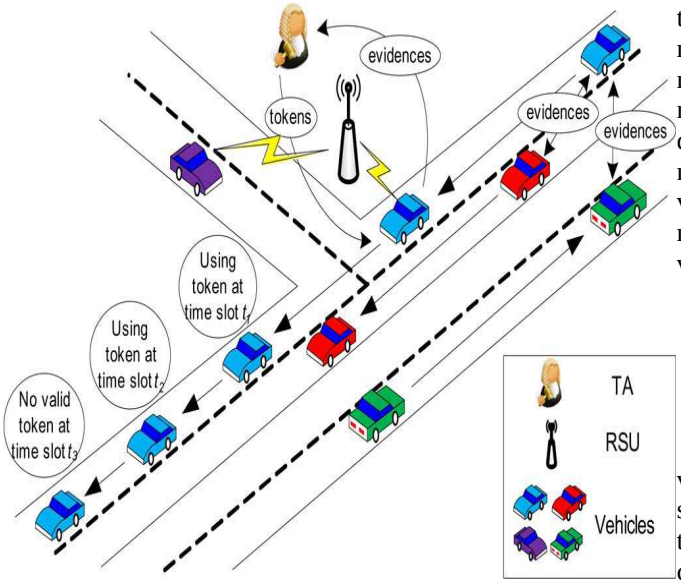


Figure 2-Proposed System Architecture

Evidence Collection by Vehicles: In step 1 of the basic scheme, a vehicle authenticates some of the original signatures that are received and generates an integrated signature at a time slot. It then creates an evidence for its authentication effort, which includes the time slot, the number of cooperative vehicles x, the number of original signatures y, and the number of original signatures vx,y that have been included in the integrated signature. It transmits the integrated signature and the evidence to others. Note that the evidence cannot be forged and will be publicly verified by the receiver vehicles. The number of evidences that are generated per vehicle should be limited. Devise a distributed approach based on geographical information for vehicles to be locally aware of their responsibilities for evidence generation. The approach randomly and fairly distributes the workload of evidence generation and minimizes the number of evidences. It also enables good vehicles to monitor potential malicious behavior.

The TA balances the contributions from and rewards toward individual users so that cooperation is largely stimulated and users are fairly treated. However, the approach cannot resist the free-riding attacks. Users are unable to distinguish a fake authentication effort from a real one, and the TA still rewards the attackers with valid tokens. Consider the free-riding attacks with fake authentication efforts (or active free-riding attack). The attackers make use of other user's authentication efforts and refuse to contribute in the cooperation.

To avoid Trusted Authority (TA) involvement to the maximum, a novel approach is proposed namely Buddy List Mechanism as a future work. Since TA acts as administrator that maintains message authentication and management of network, TA load increases due to large number of received messages. The main concept in Buddy List mechanism is to remove the direct involvement of Trusted Authority and distribute the work among the vehicle users. However, the maintenance and message authentication is done by each vehicles participating in the network. A time slot is maintained in this approach and a message is send to all vehicles during each time period.

## IV. ALGORITHM

An IBSC scheme can be used to control the capability of verification. For example, after verifying a group of original signatures, a user could encrypt an integrated signature such that others know which signatures it has verified after the corresponding decryption. Specifically, the IBSC scheme consists of the following five algorithms: setup, key generation, token generation, signcryption, and decryption and verification.

• Setup: The TA chooses G and GT to be two finite cyclic groups of the same large order q. Suppose G and GT are equipped with a pairing, i.e., a node generated and efficiently computable bilinear map e : G × G → GT such that ∀g, h ∈ G, ∀a, b ∈ Zq, e(ga, hb) = e(g, h)ab . The TA chooses generator g of group G. In addition, it also chooses random exponents β ∈ Zq and two cryptographic hash functions H : {0, 1}∗ → G and H1 : G2 → {0, 1}n. The TA sets gpub = gβ. The system public parameters are (G,GT , e, q, g, gpub,H,H1, n).

• Key Generation: The TA assigns user vi with pseudoidentity pidi with a secret key pski = Qβ i = H(pidi)β.

• Token Generation: If user vj provides enough evidences in the past time slot t − 1, the TA assigns vj with token tkt = H(t)β for time slot t.

• Signcryption: After user vi verifies a group of original signatures, it computes the following signing and encryption on message m, which denotes the group of corresponding indexes. User vi chooses a random number rs, re ∈ Zq, generates an integrated signature si,c = (s1, s2) = (grs , pski • H(m)rs ), and outputs ciphertext C = {(m_si,c) ⊕ H1(e(gre pub,H(t))), gre}.

• Decryption and Verification: If user vj has already obtained token tkt, it performs the decryption to obtain the integrated signature si,c by m_si,c = C ⊕ H1(e(gre , tkt)) and then verifies the group of indexes m by checking if e(s2, g) = e(H(pidi), gpub) • e(H(m), s1).

## V. Simulation Works/Results

To give insight into the performance of the secure cooperative authentication scheme, a set of simulations have been performed. In the following, the simulation settings and the simulation results are presented.

Simulation Settings:

Consider a relatively small and typical VANET, where vehicle users equipped with OBUs are uniformly deployed in a 10 000 m × 10 000 m area. The wireless transmission range of each OBU is 300 m. A set of 10 social spots indexed from 1 to 10, are randomly deployed into the area. At each of the four randomly selected social spots 4, 6, 8, and 10, a storage-rich RSU device with transmission radius of 1000 m is deployed, which helps users make contact with the TA. The authentication effort made by users significantly decreases as the number of users increases. By comparing the two subfigures, it is shown that, when the number of RSUs is small, the difference in required efforts decreases. When the number of vehicles increases, the effort per vehicle decreases. The figure shows that the number of vehicle is inversely proportional to the efforts per vehicle.

Simulation Results:

The Figure show the graph when the number of vehicles is 5 and the number of messages is 10.So, each user verifies 2 messages. The graph shows that the effort decreases compared to 3 vehicles. The Figure show the graph when the number of vehicles is 10 and the number of messages is also 10.So, each user verifies 1 message at a time. As the total number of users increases, the effort per vehicle decreases.

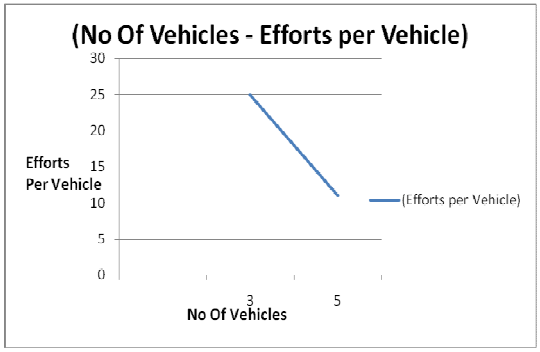


Figure 3(a) – Simulation result: 5 vehicles

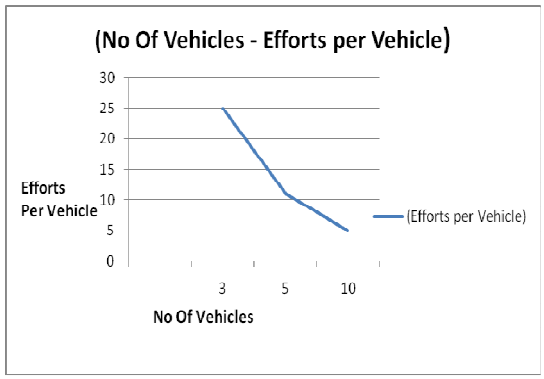


Figure 3(b) - Simulation result: 10 vehicles

The blue line shows the performance of the cooperative authentication scheme without selfish behavior. The users can obtain maximum cooperative gain since all of them behave according to the optimal approaches. The authentication effort made by users significantly decreases as the number of users increases.

Region Creation:

In web service recommender system, users usually provide QoS values on a small number of web services. Traditional memory-based CF algorithms suffer from the sparse user-contributed data set, since it's hard to find similar users without enough knowledge of their service experience. Different from existing methods, we employ the correlation between users' physical locations and QoS properties to solve this problem. In this paper, we focus on the QoS properties that are prone to change and can be easily obtained and objectively measured by individual users, such as response

time and availability. To simplify the description of our approach, we use response time (also called round-trip time (RTT)) to describe our approach.

QoS Value Prediction:

After the phase of region aggregation, thousands of users are clustered into a certain number of regions based on their physical locations and historical QoS similarities. The service experience of users in a region is represented by the region center. With the compressed QoS data, searching neighbors and making predictions for an active user can be computed quickly. Traditionally, the QoS prediction meth-ods need to search the entire data set, which is rather inefficient. In our approach, similarity between the active user and users of a region is computed by the similarity between the active user and the region center. Moreover, it is more reasonable to predict the QoS value for active users based on their regions, for users in the same region are more likely to have similar QoS experience on the same web service, especially on those region-sensitive ones.

User-collaboration Idea:

The basic idea of our approach is that users closely located with each other are more likely to have similar service experience than those who live far away from each other. Inspired by the success of Web 2.0 websites that emphasize information sharing, collaboration, and interaction, we employ the idea of user-collaboration in our web service recommender system. Different from sharing in-formation or knowledge on blogs or wikis, users are encouraged to share their observed web service QoS performance with others in our recommender system. The more QoS information the user contributes, the more accurate service recommendations the user can obtain, since more user characteristics can be analyzed from the user contributed information

Time Complexity Analysis:

The time complexity is calculating the median and MAD of each service. Form services, the time complexity. With MAD and median, we identify the region-sensitive services from the service perspective. Since there are most of 'n' records for each service, the time complexity of each service. Therefore, the total time complexity of the region-sensitive service identification.

Control centre:

Extending the previous work a control centre is designed for dynamic vehicular route choice system. It helps user to choose a trustworthy services and also provides the details about the services. It ensures the user by updating the database and guiding the user to select the Quality-Aware services when difficulties arise. It reduces the time complexity by providing an optimal value for QoS-Aware Services. Control center helps the database administrator updates the service conditions in regular intervals.

## VI. CONCLUSION

In this research work, a novel cooperative message authentication scheme for VANET is introduced. The cooperative message authentication scheme provides the ability for vehicle users to cooperatively authenticate a bunch of message pairs without the direct involvement of TA In addition, the passive free-riding attack, which are launched by selfish vehicle users, can also be effectively resisted through an evidence-token approach. Our experimental result showed that our proposed novel technique works efficiently when compared to previous methods.

## VII. REFERENCES

[1] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in Proceedings of VANET' 07, Montreal, Quebec, Canada, pp. 19–28, September 2007.

[2] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[3] H. Zhu, X. Lin, R. Lu, Pin-Han Ho, X. Shen "AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks", IEEE Trans, pp. 1436-1440, May 2008.

[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 Proc. 27th IEEE INFOCOM, Phoenix, AZ, USA, pp. 246–250, 2008.

[5] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. IEEE ICC, Beijing, China, pp. 1451–1457, May 2008.

[6] C. Zhang, X. Lin, R. Lu, P.-H. Ho and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3357-3368, 2008.

[7] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.

[8] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," in Proc. 30th IEEE INFOCOM, Shanghai, China, pp. 2147–2155, 2011.

[9] R-X Lu, X-D Lin, T-H Luan, "Pseudonym changing at social spots: an effective strategy for location privacy in VANET", IEEE Transaction on Vehicular Technology, vol. 61, no. 1, pp.86-96, Jan, 2012.

[10] X Jia, X. Yuan, L. Meng, L. Wang, "EPAS: Efficient Privacy-preserving Authentication Scheme for VANETs-based Emergency Communication", journal of software, vol. 8, no. 8, august 2013.

[11] X. Liang, R. Lu, X. Lin, and X. Shen, "PPC: Privacy-preserving chatting in vehicular peer-to-peer networks," in Proc. 72nd IEEE VTC, Ottawa, ON, Canada, pp. 1–5, 2010.
[12] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, Jan. 2007.
[13] "Veh. safety commun. project final report. Appendix H: WAVE/DSRC security," Nat. Highway Traffic Safety Admin., Washington, DC, USA, Apr. 2006.
[14] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.
[15] A. Perrig, R. Canneti, D. Song, and J. D. Tygar, "The TESLA broadcast authentication protocol," RSA Crypto., vol. 5, no. 2, pp. 2–13, 2002.
[16] X. Lin, "Secure and privacy-preserving vehicular communications," Ph.D. dissertation, Univ. Waterloo, Department of Electrical and Computer Engineering, Waterloo, ON, Canada, 2008.
[17] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On noncooperative location privacy: A game-theoretic analysis," in Proc. ACM Conf. Comput. Commun. Security, pp. 324–337, 2009.
[18] W. Susilo, F. Zhang, and Y. Mu, "Identity-based strong designated verifier signature schemes," in Proc. 9th ACISP, Sydney, Australia, pp. 313–324, 2004.

**Ranjitha P** received the bachelor's degree in Computer Science from Anna University Of Technology, 2007 and currently doing the master's degree in Calicut University, Kerala.