Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 8, August-2017, pp. 330-335 www.ijcert.org

A Novel Security Protocol for VANET

[1]B. Divya, [2]Dr. Ch. Mallikarjuna Rao
[1]*Department of Computer Science and Engineering*
Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India

[2] *Professor & Head*
Department of Computer Science and Engineering,
Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India
Email: divya.bodaa@gmail.com, chmksharma@yahoo.com

Abstract: - Vehicular ad-hoc network (VANET) has recently received significant considerations to enhance traffic security and efficiency. Notwithstanding, correspondence trust, and client protection still present useful worries to the sending of VANET, either suffer from the substantial workload of downloading the latest denial list from a remote authority or can't enable drivers made a beeline to choose the dependability of a message when the verification on messages is unknown. In this paper, to cope with these challenging concerns, we propose a new verification convention for VANET in a decentralized group model by using a new group signature scheme. In the assistance of the new group signature scheme, the proposed verification convention is featured with threshold authentication, efficient revocation, unforgeability, anonymity, and traceability. Also, the assisting group signature scheme may also be of independent interest, as it is characterized by efficient traceability and message-linkability at the same time. Broad investigations show that our proposed edge mysterious validation convention is secure, and the verification of messages among vehicles can be quickened by utilizing batch message preparing methods.

Index Terms: - Vehicular ad-hoc networks (VANETs), conditional privacy, threshold authentication, group signature

1. Introduction

Vehicular ad-hoc system (VANET), as it can give a significantly more secure, more efficient, and more open to driving background [1][2], has gotten deep consideration from both scholarly community and industry as recent. Specifically, VANET enables vehicles to talk with different vehicles, i.e., V-2-V correspondence, or roadside units (RSUs), i.e., V2-I correspondence, using the prepared onboard units (OBUs) specialized units. This kind of correspondence style (counting both V-2-V and V-2-I)[3] enables VANET to offer numerous like solace administrations and security administrations, for example, accepting traffic and weather data, and broadcasting crisis and traffic-sign-violation notices[10]. Despite its promising features, the communication trust and privacy issues in VANET should still be carefully resolved before its full flourish in real lives; otherwise, it would bring many problems, e.g., if the message broadcasted in VANET is not authenticated, then drivers cannot estimate the traffic situation according to the received messages.

If the underlying authentication method reveals the real identity of a vehicle, the location privacy of the vehicle would be disclosed.

To resolve the challenges above, many researchers have recently been devoted to planning unknown validation for VANET. Be that as it may, that current verification protocol for vanet, , either experience the suffer from the substantial workload of downloading the most recent denial list from a remote expert or can't empower drivers made a direct path to check the reliability of a message when the confirmation on messages is obscure. Potentially, the over two difficulties could be separately tackled by the decentralized group model and new verification convention technique [12],[13]. In the decentralized group model, the entire VANET is isolated into a few groups, and each group is under the control of one RSU rather than the centralized authority. In the verification convention method, receivers are permitted just to acknowledge a message that has been confirmed by a limited number of vehicles. Be that as it may, these two approaches can't be inconsequentially coordinated, as there exist two necessities for limit validation to work well in the decentralized group model,

specifically i) noticeability of message beginning which requests the capacity to check whether a similar endorser creates two unique marks on a similar message, and ii) efficient traceability which requests the capability to uncover the underwriter's personality of any mark with a little steady calculation and correspondence cost To handle the above two requirements, in this paper commendably, we will present a new anonymous authentication protocol which can well integrate the decentralized group model and threshold authentication method by using a new group signature scheme. Concretely, the main contributions of this paper are threefold.

- First, the proposed protocol employs a new group signature scheme to achieve verification and efficient traceability. Moreover, the proposed protocol also adopts the decentralized group model to release the trusted authority from the substantial load of generation of group certificates for OBUs, and to free the OBU from retrieving the denial list from the trusted authority. To the best of our knowledge, the proposed protocol is the first work that can simultaneously achieve these properties.
- Second, the proposed new group signature scheme may be of independent interest, as it is the first group signature scheme supporting efficient traceability and message linkability at the same time. In particular, it allows the tracing manager to reveal the signer's identity of any one group signature with only two exponentiations, one multiplication and one division in bilinear groups
- Finally, we likewise complete extensive investigations to demonstrate the efficiency of our proposed convention.

Group signature scheme:

Group signature [15], [16] is a special kind of digital signature, where there exist three kinds of entities: a group manager, a group tracer, and several group members. It allows group members to sign messages on behalf of the group, while nobody except the group tracer can reveal the identity of the signer. A group signature scheme is composed of the following five algorithms: SETUP, CERTGEN, SIGN, VERIFY, and OPEN. The algorithm SETUP takes the security parameter as input and outputs the public/private key pair of every entity (group manager, group tracer, group members) in the system. The algorithm CERTGEN takes the group manager's private key, public keys of a group member and the group tracer as input, and outputs a group certificate corresponding to the group of entry member's public key. The algorithm SIGN takes a group certificate, a group member's public key, and a message from message space as input, and outputs the corresponding signature. The algorithm VERIFY takes public keys of the group manager and group tracer, a message, and a signature on the message as input, and outputs 1 if the signature is valid, or 0 otherwise. The algorithm OPEN takes the group tracer's private key, a message, and a valid signature on the message as input, and outputs the public key of a group member who generates the input signature. The correctness requirement of a group signature scheme demands that honestly-generated signatures can be verified and traced correctly. On the other hand, a group signature scheme is also desired to satisfy the following three security properties: unforgeability, anonymity, and traceability. The first security property ensures that only the group member can generate signatures on be half of the group.The second security property ensures that signatures do not reveal their signer's identity except the group tracer. The third security property ensures that the group tracer can trace all valid signatures, even those generated by the collusion of multiple group members

2. Related work

Authors: P. Papadimitratos, L. Buttyan,

Critical advancements occurred in recent years in the range of vehicular correspondence (VC) [4]frameworks. Presently, it is surely known in the group that security and insurance of private client data are an essential for the sending of the innovation. This is so precisely because the advantages of VC frameworks, with the mission to upgrade transportation security and effectiveness, are in question. Without the joining of robust and functional security and protection upgrading instruments, VC frameworks could be upset or impaired even by unsophisticated assailants

This paper address this issue inside the SeVeCom extend[4], having built up a security design that gives a far-reaching and reasonable arrangement. We display our outcomes in an arrangement of two papers in this issue. In this initial one, we break down dangers and sorts of enemies, we recognize security and protection prerequisites and present a range of components to secure VC frameworks.

This paper gives an answer that can be immediately embraced and conveyed. Our advance towards usage of our design alongside comes about on the execution of the safe VC framework, are introduced in the second paper. We finish up with an examination, given current outcomes, of up and coming components to be incorporated in our protected VC engineering

Authors: G. Ateniese, J. Camenisch

Advances in remote interchanges permit setting up correspondence connects between vehicles for the trading of data between them. Such vehicular ad-hoc network (VANETs) is vital to improving activity security since basic ecological conditions, for example, street or movement conditions can be quickly traded between vehicles in VANETs. In any case, to be helpful for the driver, the data must be dependable, i.e., with incredible likelihood, the got data without a doubt mirrors the genuine circumstance.

One way to deal with this is to see data as solid if it is affirmed by different sources. To accomplish this, messages got must be recognizable. This may turn into a danger to the security of drivers since by watching messages, vehicles might be followed. In this paper, we address the said issues.

We construct the unwavering quality of data in light of the quantity of various sources that affirmed particular data, and that number must be more noteworthy than a given limit. We address the traceability by giving vehicles a chance to change their personality as often as possible. Our approach scales concerning capacity on the vehicle, and also administration of personalities at a confirmation specialist.

Author: L. Zhang, Q. Wu

Existing verification conventions to secure vehicular ad-hoc network (VANETs) raise difficulties, for example, declaration dissemination and renouncement, evasion of calculation and correspondence bottlenecks, and lessening of the solid dependence on sealed gadgets.

This paper effectively adapts to these difficulties with a decentralized gathering verification convention[12] as in the gathering is kept up by every roadside unit (RSU) instead of by a real expert, as in most existing conventions that are utilizing bunch marks. In our proposition, we utilize each RSU to keep up and deal with an on-the-fly gathering inside its correspondence run.

Vehicles entering the gathering can secretly communicate vehicle-to-vehicle (V2V) messages, which can be in a flash checked by the vehicles in a similar rally (and neighboring gatherings). Afterward, if the message is observed to be false, an outsider can be summoned to reveal the personality of the message originator.

Existing system:

Our convention productively misuses the particular elements of vehicular versatility, physical street impediments, and appropriately circulated RSUs. Our outline prompts a vigorous VANET since, if some RSUs incidentally fall, just the vehicles that are driving in those collapsed areas will be influenced. Due to the various RSUs sharing the load to keep up the system, execution does not decrease when more vehicles join in the VANET; consequently, the system is adaptable

To determine the previously mentioned challenges, many research endeavors have recently committed to outlining unknown confirmation for VANET. Be that as it may, those existence verification conventions for VANET either experience the suffer from the substantial workload of downloading the newest denial list from a remote expert, or can't enable drivers making a course for choose which message is valid or not.

Potentially, the over two difficulties could be individually settled by the decentralized group model and limit verification strategy. In the decentralized group model, the entire VANET is isolated into a few groups, and each group is under the control of one RSU rather than the central authority. In the verification convention, beneficiaries are permitted just to acknowledge a message that has been affirmed by an edge number of vehicles.

The impediments of existing system is the two procedures cannot be trivially incorporated, as there exist two prerequisites for limit confirmation to function admirably in the decentralized gathering model, in particular

i) Distinguish capacity of message birthplace which requests the ability to check whether a similar endorser produces two unique marks on a similar message, and

ii)Efficient traceability which requests the capacity to uncover the underwriter's personality of any mark with a little steady calculation and correspondence cost

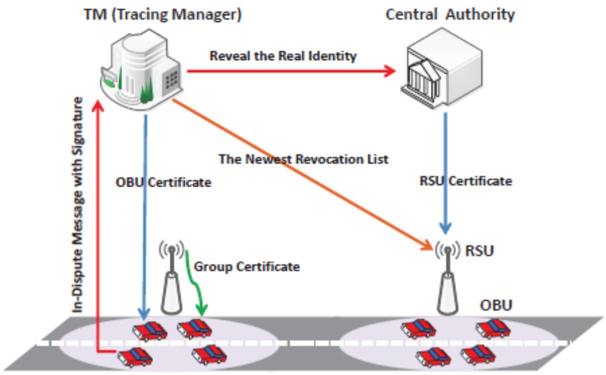
3. Proposed system

To overcome above-mentioned problems we present a new verification convention method which can well integrate the decentralized group model and threshold authentication method by using a new group signature scheme.

- First, the proposed protocol employs a new group signature scheme to achieve verification convention and efficient traceability. Moreover, the proposed protocol also adopts the decentralized group model to release the trusted authority from the substantial burden of a generation of group certificates for OBUs, and to free the OBU from retrieving the denial list from the trusted authority. To the best of our knowledge, the proposed protocol is the first work that can simultaneously achieve these properties.
- Second, the proposed new group signature scheme may be of independent interest, as it is the first group signature scheme supporting efficient traceability and message likability at the same time. Specifically, it enables the following chief to uncover the underwriter's character of any one gathering mark with just two exponentiations, one increase and one division in bilinear gatherings.
- Finally, we also carry out extensive analyses to show the efficiency of our proposed protocol

The Proposed System had the extensive performance for VANET.

4. Architecture



Our architecture demonstrates made out of the accompanying gatherings: the focal specialist (CA), the following tracer (TM), many RSUs, and numerous OBUs, as appeared in Fig. The CA is in charge of confirming general society keys of RSUs. After confirmation, the CA will issue the key certificates. The TM is responsible for confirming the public keys of OBUs. After validation, the TM will issue the key certificates. The TM is likewise ready to give the sender the identity who communicates a false/in-question message in the system. RSUs are dispersed along the street and intended to deal with a group of OBUs similar range. Particularly, every RSU will issue each OBU inside its correspondence go a gathering certificate that is utilized together with OBU's private key to sign the communicated message in the related group. Every vehicle is mounted with an OBU, and the OBU can ask for group certificates from RSUs and communicate with each other given the devoted short-range communication rule [12]. The OBU acknowledges one message if and just if there are a sufficient number of valid signatures on the message. The number could be balanced on the off chance that the OBU wishes. Note that RSUs will not issue the group certificate to the OBU which has existed in the denial list managed by the TM

Threshold authentication:

The use of the threshold authentication method to achieve some assurance of trueness on the received traffic information is a common approach in many works. The threshold value in the threshold authentication method may be fixed by the system or dynamic according to user’s willing. One key issue to use the threshold authentication method is the distinguishability of message origin. That is, two signatures on the same message by the same signer should be linkable by anyone.

The OBU can change the threshold at anytime. Distinguishability of message origin anyone can check whether the same signer generates two different signatures on the same message

Efficient revocation:

The TM can reveal the signer’s identity of anyone signature with constant computation and communication cost. Furthermore, the OBU does not need to retrieve the newest revocation list from the remote CA or TM.

Unforgeability:

Only the OBU holding the group certificate from one RSU can generate valid signature on behalf of the group that is maintained by the RSU

Anonymity and Traceability:

Only the TM can reveal the signer’s identity. In other words, even RSUs, they cannot reveal any OBU’s location if the OBU is not in their communication range Any OBU cannot generate any valid signature which is traced back to other OBU

5. Conclusion

In this paper, we have 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, unforgeability, anonymity, and traceability for VANETs. Also, the newly proposed group signature scheme may also be of independent interest, as it is the first one supporting efficient traceability and message-likability. In our future work, we will further improve the effectiveness of the batch verification in VANET. In particular, we plan to design a new protocol in which the computational cost of pairing in batch verification is constant.

References

[1] Jun Shao, Xiaodong Lin, "A threshold anonymous authentication protocol for valet"

[2] S. Dietzel, E. Schoch, B. K¨onings, M. Weber, and F. Kargl, "Resilient, secure aggregation for vehicular networks," IEEE Network, vol. 24, no. 1, pp. 26–31, 2010. [Online]. Available: http://dx.doi.org/10.1109/ MNET.2010.5395780

[3] "The car two car communication consortium," http://www.car-to-car.org/.

[4] P. Papadimitratos, L. Butty´an, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. Hubaux, "Secure vehicular communication systems: Design and architecture," CoRR, vol. abs/0912.5391, 2009. [Online]. Available: http://arxiv.org/abs/0912.5391

[5] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings, 2000, pp. 255–270. [Online]. Available: http://dx.doi.org/10.1007/3-540-44598-6 16

[6] J. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security & Privacy, vol. 2, no. 3, pp. 49–55, 2004. [Online]. Available: http://doi.ieeecomputersociety.org/10.1109/ MSP.2004.26

[7] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007. [Online]. Available: http://iospress.metapress.com/openurl.asp?genre= article&issn=0926-227X&volume=15&issue=1&spage=39

[8] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," IEEE T. Vehicular Technology, vol. 59, no. 7, pp. 3589–3603, 2010. [Online]. Available: http: //dx.doi.org/10.1109/TVT.2010.2051468

[9] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," IEEE T. Vehicular Technology, vol. 62, no. 7, pp. 3339–3348, 2013. [Online]. Available: http://dx.doi.org/10.1109/TVT.2013.2257188

[10] L. Wischhof, A. Ebner, and H. Rohling, "Information dissemination in self-organizing intervehicle networks," IEEE Transactions on Intelligent Transportation Systems, vol. 6, no. 1, pp. 90–101, 2005. [Online]. Available: http://dx.doi.org/10.1109/TITS.2004.842407

[11] P. Golle, D. H. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in Proceedings of the First International Workshop on Vehicular Ad Hoc Networks, 2004, Philadelphia, PA, USA, October 1, 2004, 2004, pp. 29–37. [Online]. Available: http://doi.acm.org/10.1145/1023875.1023881

[12] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE T. Vehicular Technology, vol. 59, no. 4, pp. 1606–1617, 2010. [Online]. Available: http://dx.doi.org/10.1109/TVT.2009.2038222

[13] L. Chen, S. Ng, and G. Wang, "Threshold anonymous announcement in vanets," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 605–615, 2011. [Online]. Available: http: //dx.doi.org/10.1109/JSAC.2011.110310

[14] U. S. D. of Transportation, "Dedicated short range communications," http://www.its.dot.gov/DSRC/.

[15] D. Chaum and E. van Heyst, "Group signatures," in Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings, 1991, pp. 257–265. [Online]. Available: http://dx.doi.org/10.1007/3-540-46416-6 22

[16] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 1519, 2004, Proceedings, 2004, pp. 41–55. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-28628-8 3

[17] Anusha.V,K.Sumalatha," Mobile Social Networks for Flattering Unsigned Profile Matching ," International Journal of Computer Engineering In Research Trends.,vol.1,no.6,pp. 384-390,2014.

[18] D.Ramanjaneyulu ,U.Usha Rani," In Service-Oriented MSN Providing Trustworthy Service Evaluation," International Journal of Computer Engineering In Research Trends.,vol.2,no.12,pp. 1192-1197,2015.

[19] Komal Patil, Geeta Mahajan, Disha Patil and Chitra Mahajan," Implementation of Motion Model Using Vanet," International Journal of Computer Engineering In Research Trends.,vol.3,no.4,pp. 179-182,2016.

[20] Pocha Nageswara Reddy, I.S.Raghuram, Dr.S.Prem Kumar," Advance EMAP for Vehicular Ad Hoc Networks." International Journal of Computer Engineering In Research Trends.,vol.1,no.4,pp. 253-258,2016.