International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Review on Message Authentication Protocol for Vehicular Ad Hoc Network

Sarika A. Velukar[1], Dr. M. S. Ali[2]

[1]Prof. Ram Meghe College of Engineering and Management, Amravati University, Amravati, India
[2]Prof. Ram Meghe College of Engineering and Management, Amravati University, Amravati, India

Abstract: ***Intelligent Transportation Systems are aimed at addressing critical issues like passenger safety and traffic congestion, by integrating information and communication technologies into transportation infrastructure and vehicles. They are built on top of self organizing networks, known as a Vehicular Ad hoc Networks (VANET), Vehicular communication systems facilitate communication devices for exchange of information among vehicles and between vehicles and roadside equipment. As vehicles communicate through wireless network, variety of attacks can take place like injecting false information and modifying messages. A security attack on VANETs can have severe harmful or fatal consequences to legitimate users. So there is need to have secure vehicular communications. A novel solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. For this purpose a new Message Authentication Protocol is proposed for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The revocation check process uses a keyed Hash Message Authentication Code. This new protocol significantly decrease the message loss ratio due to the message verification delay and end to end delay compared with the conventional authentication methods employing CRL.***

Keywords: Vehicular Ad Hoc Network (VANET), Public Key Infrastructure (PKI), Certificate Revocation List (CRLs), Authentication.

1. Introduction

A Vehicular Ad-hoc Network (VANET) is a communication network for vehicles on the road. The vehicles are equipped with the required hardware/software that gives them the cleverness to communicate with each other. This feature enables a range of applications to improve transportation safety and efficiency. Vehicular networks (VNs) are emerging as a convincing instantiation of the mobile networking technology among civilian applications. However, security is a critical factor and a significant challenge to be met. In a VANET, each vehicle is equipped with the technology that allows the vehicle to communicate with each other as well as with the roadside infrastructure, e.g., base stations also known as roadside units (RSUs), located in some critical sections of the road, such as traffic lights, intersections, or stop signs, to improve the driving experience and make driving safer. By using such communication devices, also known as on-board units (OBUs), vehicles can communicate with each other as well as with RSUs. A VANET is a self-organized network that enables communications between vehicles and RSUs, and the RSUs can be connected to a backbone network, so that many other network applications and services, including Internet access, can be provided to the vehicles.

As vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the dispersed messages can be easily launched. A security attack on VANETs can have severe harmful penalty to legal users. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL is a list containing all the revoked certificates issued by a Trusted Authority (TA). In a PKI system, the message is authenticated by first checking if the sender's certificate is included in the current CRL i.e. by first checking its revocation status after that verifying the sender's certificate and then lastly verifying the sender's signature on the received message. The first part of the authentication may incur long delay depending on the CRL size and the employed mechanism for searching the CRL. Unfortunately, the CRL size in VANETs is expected to be large for the following reasons: 1) To preserve the privacy of the drivers and location information of the drivers from any external eavesdropper [1], [2], [3]. 2) The scale of VANET is very large.

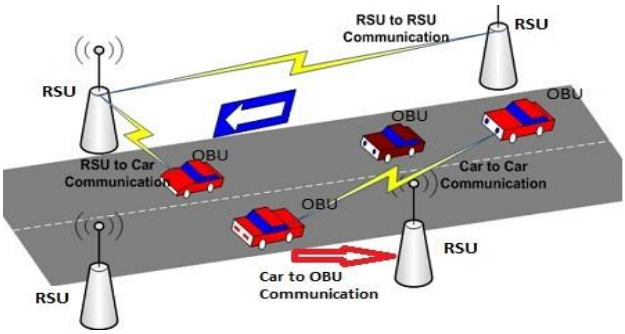

Figure 1: VANET Structure

2. Motivation

According to the Dedicated Short Range Communication (DSRC) [7] each OBU has to broadcast a message every 300 msec about its location, and other information. In such scenario, each OBU may receive a large number of messages every 300 msec, and it has to check the current CRL for all the received certificates, which may incur long

authentication delay depending on the CRL size and the number of received certificates. The ability to check a CRL for a large number of certificates in a timely manner leads an unavoidable confront to VANETs. To guarantee trustworthy operation of VANETs and increase the amount of authentic information gained from the received messages, each OBU should be able to check the revocation status of all the received certificates in a timely manner. So there is a need to reduce authentication delay while authenticating messages from vehicle. And this can be gain by reducing the authentication delay in checking CRLs in VANET.

3. Literature Survey

We are witnessing an inimitable junction of Vehicular Ad-hoc Networks (VANET) and Intelligent Transportation Systems (ITS) which is on the edge to bring about a innovatory leap by making our roadways and streets safer and the driving experience more enjoyable. Working with the fielded ITS infrastructure, VANET is expected to improve the consciousness of the travelling public by aggregating, propagating and disseminating *up-to-the-minute* information about coming traffic-related events. In VANETs, the key security requirements are recognized as entity authentication, message integrity, non-repudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirements [4], [9]. PKI employs CRLs to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long.

In [9], Hubaux identify the specific issues of security and privacy challenges in VANETs, and designate that a PKI should be well deployed to protect the transited messages and to communally authenticate network entities.

In [4], Raya and Hubaux have explained why vehicular networks need to be secured, and why this problem requires a specific approach. They have proposed a model that identifies the most relevant communication aspects; and have also identified the major threats. They have then proposed security architecture along with the related protocols. Authors have used a classical PKI to provide secure and privacy preserving communications to VANETs. In this approach, each vehicle needs to preload a huge pool of anonymous certificates. The number of the loaded certificates in each vehicle should be large enough to provide security and privacy preservation for a long time, e.g., one year. Each vehicle can update its certificates from a central authority during the annual inspection of the vehicle. In this approach, revoking one vehicle implies revoking the huge number of certificates loaded in it.

In [10], Studer et al. propose an efficient authentication and revocation scheme called TACK. Temporary Anonymous Certified Keys (TACKs) is an efficient way to fulfill the security and privacy properties necessary for key management in Vehicular Ad Hoc Networks (VANETs). In TACKs, On-Board Units (OBUs) use short-lived keys to sign messages used for VANET communication. These short-lived keys are certified by Regional Authorities (RAs). During key updates, RAs verify that the requesting OBU is a legitimate OBU that has not been revoked; however, the RAs do not learn the OBU's identity. This allows a valid OBU to acquire a certificate for a temporary key and preserve the OBU's privacy. Since RAs' certificates are only valid in their local region, OBUs must update keys upon entering a new region. When a set of OBUs enters the region, all of the OBUs update keys simultaneously, preventing eavesdroppers from tracking drivers across key changes. If a message is identified as an abuse of the VANET, authorities can trace the certificate request back to the signer. The authorities can revoke the misbehaving OBU so that it is no longer able to participate in the VANET.

TACK adopts a hierarchy system architecture consisting of a central trusted authority and regional authorities (RAs) distributed all over the network. The authors adopted group signature where the trusted authority acts as the group manager and the vehicles act as the group members. Upon entering a new region, each vehicle must update its certificate from the RA dedicated for that region. The vehicle sends a request signed by its group key to the RA to update its certificate; the RA verifies the group signature of the vehicle and ensures that the vehicle is not in the current Revocation List (RL). After the RA authenticates the vehicle, it issues short lifetime region-based certificate. This certificate is valid only within the coverage range of the RA. It should be noted that TACK requires the RAs to wait for some time, e.g., 2 seconds, before sending the new certificate to the requesting vehicle. This renders the vehicle not able to send messages to neighboring vehicles within this period, which makes TACK not suitable for the safety applications in VANETs as the WAVE standard [6] requires each vehicle to transmit beacons about its location, speed, and direction every 100-300 msec. Also, TACK requires the RAs to completely cover the network; otherwise, the TACK technique may not function properly. This requirement may not be feasible especially in the early deployment stages of VANETs. Although TACK eliminates the CRL at the vehicles level, it requires the RAs to verify the revocation status of the vehicles upon requesting new certificates. To check the revocation status of a vehicle, the RA has to verify that this vehicle is not in the current RL by performing a check against all the entries in the RL. Each check requires three pairing operations. Consequently, checking the revocation status of a vehicle may be a time consuming process. The authors suggested to use an optimized search method to remedy the computationally expensive RL check. The proposed method can reduce the RL checking to two pairing operations. However, this solution is based on fixing some parameters in the group signature attached to every certificate request, which reduces the privacy preservation of TACK and renders the tracking of a vehicle possible. There are some works addressing the problem of distributing the large-size CRL in VANETs.

In [11], Raya et al. introduce a framework to thwart internal attackers in vehicular networks. The eviction of faulty or attacking nodes is crucial to the robustness of

vehicular communication systems. As revocation is the primary means to achieve this, authors have designed two protocols tailored to the characteristics of the VN environment. Authors have also designed a scheme that can robustly and efficiently achieve isolation of misbehaving and faulty nodes, as well as contribute to their eventual revocation. This is done with the help of a misbehavior detection module and a distributed eviction protocol. These protocols together cover the whole spectrum of VN scenarios. Authors have also introduced Revocation using Compressed Certificate Revocation Lists (RC2RL), where the traditional CRLs, issued by the TA, are compressed using Bloom filters to reduce its size prior to broadcasting.

Papadimitratos et al. [12] presented a simple and robust design for CRL distribution in VC systems, leveraging on VC equipment that is to be deployed. Authors found that with very low bandwidth used for CRL transmissions, practically all vehicles can obtain the latest CRL within tens of minutes, e.g., the duration of a commute. Analysis reveals trade-offs and how the system can be configured to reduce the CRL acquisition delay. Overall, scalability is achieved due to keeping CRL sizes low and due to minimal RSU-CA and no RSU-RSU interactions. Authors propose to partition the CRL into small pieces and distribute each piece independently.

Laberteaux et al. [13] use car to car communication to speed up the CRL broadcasting.

Haas et al. [5] have made two contributions in this paper. First, authors proposed a certificate organization method where certificates for a single vehicle are related by a single, secret revocation key. Without this key, certificates are difficult to group, thereby preserving the privacy of a vehicle. However, a revoked vehicle's certificates can be easily identified once the revocation key is distributed via a CRL. To revoke a new vehicle, the CRL need only increase in size by one revocation key, regardless of the number of certificates provided to the revoked vehicle. They presented specific privacy properties of this scheme. Second, authors have analyzed and improved the practicality of distributing CRLs. Authors proposed a mechanism for passing CRL updates, rather than the entire CRL, which reduces the imposed network overhead and is similar to delta CRLs. Together, these contributions demonstrate that a lightweight privacy preserving method for VANET security is possible, even in the case of sparse roadside infrastructure. They have develop a mechanism to reduce the size of the broadcast CRL by only sending a secret key per revoked vehicle. On receiving the new CRL, each OBU uses the secret key of each revoked vehicle to reproduce the identities of the certificates loaded in that revoked vehicle, and construct the complete CRL. It should be noted that although the broadcast CRL size is reduced, the constructed CRL at each OBU, which is used to check the revocation status of other entities, still suffers from the expected large size exactly as that in the traditional CRLs where all the identities of the certificates of every revoked OBU are included in the broadcast CRL. Also, the authors propose using bloom filter, which is some kind of lookup hash tables, to perform CRL checking for the received certificates. To minimize the false-positives in the bloom filter, the authors proposed that each vehicle has to check before sending its certificate whether this certificate will trigger a false positive or no. If yes, then it uses another certificate. The authors proposed to upload each vehicle with additional certificates to compensate for those ones which will trigger a false positive. Although this solution can minimize the false positives, it cannot to completely prevent them, which limits their advantages, especially, in safety-related VANETs applications. The probabilistic approach is a promising technique for the key management in ad hoc networks [14], [15].

Zhu et al. introduce the GKMPAN protocol [16], scalable and efficient group key management protocol for ad hoc networks. This protocol is based on a probabilistic key sharing scheme that can be parameterized to meet the appropriate levels of security and performance for the application under consideration. The main component of GKMPAN is a novel group rekeying protocol that is efficient, scalable and partially stateless. This protocol adopts a probabilistic key distribution approach which i based on pre-deployed symmetric keys. In [17], a probabilistic random key distribution is proposed to achieve efficient privacy-preserving group communication protocol for VANETs. Employing a probabilistic random key distribution and a secret key sharing threshold scheme, an efficient distributed revocation protocol for VANET is designed in [18].

Albert Wasef, and Xuemin Shen in [18] have proposed a robust EDR protocol for VANETs that substantially reduces the complexity of the certificate revocation problem while achieving fast revocation of the misbehaving vehicles. The EDR protocol decreases the vulnerability window that a misbehaving vehicle has, resulting in a higher safety level for VANET. The EDR protocol is resistant to the most known revocation attacks. In addition, it can efficiently be integrated with any PKI and/or any misbehavior detection scheme for VANETs.

4. Comparative Study

Sr. No	*Methodology*	*Performance Evaluation*	*Author's claim*	*Our Findings*
1	Classical PKI [4]	Compliance with the security requirements, Anonymity	Security solutions to be deployed in VANET	Digital signature used as authentication mechanism
Sr. No	Methodology	Performance Evaluation	Author's Claim	Our Findings
2	TACK [10]	Message integrity, Traceability and Revocability	Efficient Authentication scheme	Fulfills security and privacy polices
3	Lightweight Mechanism for revoking certificates [5]	False positives	Mechanism to distribute updated CRLs	Low overhead
4	RC2RL,MDS [11]	Average speed, Vehicle Density	Revocates misbehaving and faulty nodes	Thwart internal attackers in network
8	Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks [16]	Communication cost	Meet appropriate level of security and performance by using probabilistic key sharing	Efficient and scalable protocol
6	Certificate Revocation List Distribution in Vehicular Communication Systems [12]	Acquisition Delay	Distribution of large CRLs across wide VC regions within minutes	Scalability is achieved
7	Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks [8]	Authentication delay, end to end delay	Efficient revocation checking process over existing	Resistance to attack
8	An Efficient Distributed Certificate Service Scheme for VANET [18]	OBU certificate update delay, OBU message signing delay	Three new mechanisms for key establishment	Improves security but at the cost of communication overhead
9	Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks [18]	Feasibility and reliability	Reduces the complexity of the certificate revocation problem while achieving fast revocation of the misbehaving vehicles	Decreases vulnerability window and increases safety level

We have done a detailed study of various approaches related to the message authentication protocol in VANET and identified their implementation techniques. Then we had performed a comparative analysis on them to identify their limitations. Most of the Protocol which we have study overcome the authentication issue but they are at the cost of computation overhead.

By the above study and analysis, we come to know that many of the approaches are still not efficient for message authentication. For a fully secure network, we will implement a new Protocol for message authentication in VANET based on hashed message authentication code HMAC. Firstly we will do system initialization and then message authentication will be done in two stages, first by message signing and then by message verification after that revocation. Lastly we will perform comparative analysis with existing system.

5. Conclusion

In this paper we have reviewed different existing protocols and techniques or message authentication in Vehicular Ad hoc Network. By analyzing the existing system we will propose a new message authentication protocol based on hashed message authentication code to reduce delay in authentication process while vehicular communication. We will perform comparative analysis on parameters like throughput, end to end delay, message digest generation with existing system.

References

[1] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: A Position

Paper," Proc. Workshop Standards for Privacy in User- Centric Identity Management, July 2006.
[2] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing Location Privacy for VANET," Proc. Embedded Security in Cars (ESCAR) Conf., Nov. 2005.
[3] A. Wasef, Y. Jiang, and X. Shen, "DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.
[4] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.
[5] J.J. Haas, Y. Hu, and K.P. Laberteaux, "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET," Proc. Sixth ACM Int'l Workshop VehiculAr InterNETworking, pp. 89-98, 2009.
[6] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.
[7] 5.9 GHz DSRC," http://grouper.ieee.org/groups/scc32/dsrc/ index.html, 2012.
[8] A. Wasef and X. Shen, "MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks," Proc. IEEE GlobeCom, 2009.
[9] J.P. Hubaux, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.
[10] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09), pp. 1-9, 2009.
[11] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1557-1568, Oct. 2007.
[12] P.P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate Revocation List Distribution in Vehicular Communication Systems," Proc. Fifth ACM Int'l Workshop VehiculAr Inter-NETworking, pp. 86-87, 2008.
[13] K.P. Laberteaux, J.J. Haas, and Y. Hu, "Security Certificate Revocation List Distribution for VANET," Proc. Fifth ACM int'l Workshop VehiculAr Inter-NETworking, pp. 88-89, 2008.
[14] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 197-213, 2003.
[15] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security, pp. 41-47, 2002.
[16] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks," J. Computer Security, vol. 14, pp. 301-325, 2006.
[17] A. Wasef and X. Shen, "PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1458-1463, 2008.
[18] A. Wasef and X. Shen, "EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 9, pp. 5214-5224, Nov. 2009