International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 08
July 2017

Secure And Authenticated Message Dissemination In VANETS

Divya Boya[1], Sravya Boya[2]
[1]*Assistant Professor, Arjun College of Technology and Science*
[2]*Assistant Professor, Arjun College of Technology and Science*

Abstract: Vehicular advert hoc Networks (VANETs) enable automobiles to form a self-geared up network. VANETs are likely to be widely deployed someday, given the curiosity shown with the aid of enterprise in self-driving automobiles and pleasurable their patrons various pursuits. In this paper, we suggest an Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-drinking CRL checking process via an efficient revocation checking approach. The revocation assess system in EMAP makes use of a keyed Hash Message Authentication Code (HMAC), where the key utilized in calculating the (HMAC) is shared simplest between non-revoked OBUs. Additionally, EMAP makes use of a novel probabilistic key distribution, which makes it possible for non-revoked OBUs to soundly share and replace a secret key. EMAP can drastically scale down the message loss ratio because of the message verification prolong in comparison with the traditional authentication methods employing CRL. By way of conducting security evaluation and performance analysis, EMAP is validated to be comfortable and efficient.

Keyword-Vehicular networks, Communication security, Message authentication, Certificate revocation.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) provide ubiquitous connectivity to mobileusers on the road and efficient vehicle-to-vehicle communication that can help inimplementing Intelligent Transportation Systems (ITS). ITS can provide support forvarious types of applications such as collision prevention, traffic monitoring, trafficflow control, providing information about nearby services. Another importantapplication of VANETs is that since vehicles are connected to the Internet, the userscould enjoy the services, the infotainment, and the entertainments, supported on theInternet while they are moving.VANETs are special type of MANETs (Mobile Ad hoc Networks). The maindifference between the two is that nodes in VANETs are vehicles on the roadway andtheir movement is constrained to roads whereas nodes in MANETs move randomly.One of the primary goals of VANETs is to increase road safety. In order to achievethis goal, vehicles monitor phenomena on the roads and inform other vehicles aboutabnormal and dangerous traffic condition such as icy roads, heavy congestion, or caraccidents. Adversaries could exploit this by injecting malicious messages for theirown benefit or to deliberately disrupt the users. Thus, securing VANETs from such

adversaries is important.In VANETs, each vehicle is equipped with a communication device to communicate with other vehicles and designated roadside infrastructure, called road side units,to exchange safety related information. These vehicle nodes and roadside infrastruc-ture together form a self-organized network, called a Vehicular Adhoc Network. InVANETs, various type of techniques are required such as beaconing, forwarding,broadcasting, and routing to deliver messages to the destination through appropriate nodes. Due to the high mobility of vehicle nodes, the network topology changes frequent.

Two types of communicating entities are presented in the currently explored architectures of VANETs. The first type is a vehicle node which forms the majority ofall VANET nodes.The second type is the roadside base stations, usually called RSUs(Road Side Units). The radio used for communication is Dedicated Short-Range Communications (DSRC), which has been allocated as a new band in 1999 by the

FederalCommunications Commission; the band allocated was 75MHz at 5.9GHz frequencyfor Intelligent Transport System(ITS) applications in North America. Also, the IEEE802.11p standard supports the communication channel and technology. Communication in VANETs could be either direct communication between vehicles or throughmultiple wireless link hops. Vehicles operate as both endpoints and routers. Vehicularnetworking will enable vehicle-to-vehicle communication, vehicle-to-RSU communication, and vehicle-to-existing infrastructure networks communication.

High velocity of vehicle is a real-time constraint in VANETs. For example, iftwo vehicles are moving in opposite direction on highways, they would only have avery short connection time between them. Also, unlike MANETs in which nodesmove randomly, vehicles move along the roads, hence their mobility is constrained.Vehicles in VANET are equipped with a wireless communication device and computation resources to perform security tasks. Also, additional devices such as a GlobalPositioning System (GPS) and an Event Data Recorder (EDR) could be present toprovide the location of vehicles. Vehicles also have a tamper-proof storage for privateinformation such as private/public keys and electronic license plate information.

II. RELATED WORK

Trusted authority (TA)

In VANETs trusted authority is an essential entity which provides identity for vehicles and monitors the entire networkand other the major responsibility of the trusted authority is public key management. Public key management includes public keyregistration, public key publication, and public key revocation processes. It is also responsible for issuing the secret keys to thevehicles.

Road side Units (RSU):

RSUs are stationary devices placed in critical locations of the road (e.g. junctions) capable of communicating withvehicles and the backbone network. RSUs are collaborating in VANETs by distributing/collecting traffic and non-traffic related information to/from vehicles and by providing different features to manage the system. In other words, RSUs works as aninterface between the backbone infrastructure and the vehicles. One interesting application of RSUs is to recommend optimizedspeed to vehicles approaching to junctions equipped with traffic lights. This will let the driver pass the junction without stoppingand smoothing the traffic which will increase efficiency (e.g. fuel consumption of heavy vehicles can be dropped drastically)

On board units (OBU):

In VANET, vehicles are equipped with devices called OBU, capable of communicating with RSUs and other nearbyOBUs. OBU frequently broadcasts messages including information about the vehicle position, speed, direction, braking statusand other related information associated to the vehicle. OBUs in collaboration with vehicle sensors can compute and generate avariety of messages upon different situations (e.g. emergency braking, traffic jams, accidents and change in weather condition)Each OBU is equipped with a Hardware Security Module (HSM), which is a tamper-resistant module used to store thesecurity materials, e.g., secret keys, certificates, etc., of the OBU. Also, the HSM in each OBU is responsible for performing allthe cryptographic operations such as signing messages, verifying certificates, keys updating, etc.

Figure.1 is describing thetwo main types of communication modes in VANETs: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-RoadsideInfrastructure (V2I) communication. In V2V communication mode a vehicle communicates with other vehicles present in thenetwork and all the vehicles engaged in the communication are mobile. V2I communication refers to a type of communicationthat involves Road Side Units (RSUs) communicating with the vehicles

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 08
July 2017

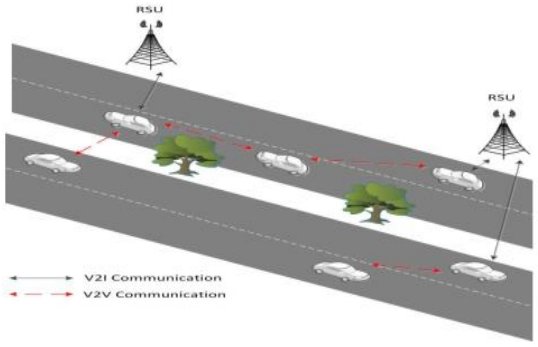

Figure 1 Communication modes in VANETs

In VANETs, the primary security requirements are identified as entity authentication, message integrity, nonrepudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirements [11], [12].PKI employs CRLs to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay ofchecking the revocation status of a certificate included in a received message is expected to be long.In [13], the technique was used to identify the specific issues of security and privacy challenges in VANETs, andindicate that a PKI should be well deployed to protect the transited messages and to mutually authenticate network entities. Inthis approach, each vehicle needs to preload a huge pool of anonymous certificates. The number of the loaded certificates in eachvehicle should be large enough to provide security and privacy preservation for a long time, e.g., one year. Each vehicle canupdate its certificates from a central authority during the annual inspection of the vehicle. In this approach, revoking one vehicleimplies revoking the huge number of certificates loaded in it.

In [12], an efficient authentication and revocation scheme called TACK is proposed. TACK adopts a hierarchy systemarchitecture consisting of a central trusted authority and regional authorities (RAs) distributed all over the network. Here groupsignature concept is adopted, 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 arequest signed by its group key to the RA to update its certificate ,the RA verifies the group signature of the vehicle and ensuresthat the vehicle is not in the current Revocation List (RL). After the RA authenticates the vehicle, it issues short lifetime regionbased certificate. This certificate is valid only within the coverage range of the RA. It should be noted that TACK requires theRAs to wait for some time, e.g., 2 seconds, before sending the new certificate to the requesting vehicle. This renders the vehiclenot able to send messages to neighboring vehicles within this period, which makes TACK not suitable for the safety applicationsin VANETs.

A different way of reducing the size of the CRL involves using types of compression techniques. One method forcompressing the CRL information using Bloom filters was introduced by in [14] . In this method, each certificate that is revokedis hashed to a fixed number of bits several times. The resulting hash value for each revoked certificate forms a type of signature.The signatures of several revoked certificates can be combined into a single bit sequence that serves as the Bloom filter. Eachtime a certificate is received, the same hashes are performed and the resulting value is checked against the Bloom filter. If thesignature matches a pattern in the Bloom filter, that means the certificate has been revoked with high probability. Storing CRLinformation in this manner compresses the size of the CRL considerably since a fixed-length Bloom filter is distributed insteadof distributing 8 to 14 bytes for every certificate that is revoked.

III. PROPOSED WORK

The main aim of this project is to develop an architectural framework to authenticate bulk messages in VANETsusing EMAP. The proposed system ensures low end-to-end delay, low overhead and thus a better communicationchannel. The EMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random keydistribution. Expedite Message Authentication Protocol (EMAP) to overcome the problem of the long delay incurred inchecking the revocation status

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 08
July 2017

of a certificate using a CRL. EMAP employs keyed Hash Message Authentication Code[HMAC] in the revocation checking process, where the key used in calculating the HMAC for each message is sharedonly between unrevoked OBUs. In addition, EMAP is free from the false positive property which is common for lookuphash tables. Extension of EMAP for bulk authentication in VANETs clearly reduces the communication overheadthereby making the communication faster and easier.

As shown in the figure the system model consists of the following:

- A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to allOBUs in the network.
- Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicatesecurely with the TA.
- OBUs, which are embedded in vehicles. OBUs can communicate either with other OBUs through V2Vcommunications or with RSUs through V2I communications.

1. Computation Complexity of Revocation Status Checking

In EMAP, the revocation checking process requires only one comparison between the calculated and received valuesof REVcheck. As a result, the computation complexity of EMAP is O(1), which is constant and independent of thenumber of revoked certificates. In other words, EMAP has the lowest computation complexity compared with the CRLchecking processes employing linear and binary search algorithms.

2. Authentication Delay

The message authentication delays are employed in checking the revocation status of the OBU units. The authentication messages are performed by three processes: checks the sender revocation status, verify the sendercertificate and also check the sender signature. For VANET the CRL adopt secure hash algorithm by encrypting themessage. For the second and third authentication phases, we employ Elliptic Curve Digital Signature Algorithm(ECDSA) to check the authenticity of the certificate and the signature of the sender. ECDSA is the digital signaturemethod chosen by the WAVE standard.

3. End -to- end delay

The end-to-end delay is defined as the time to transmit a message from the sender to the receiver.

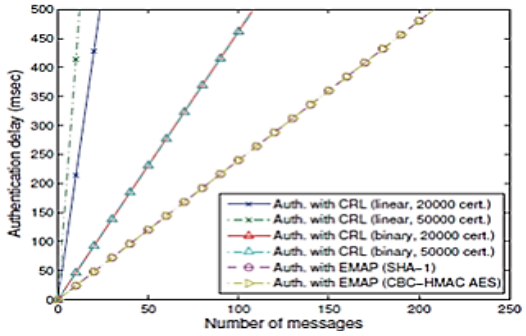

Fig: 2 Authentication Delay per message

It can be seen that the end-to-end delay increases with the OBUs density because the number of the received packetsincreases with the OBUs density resulting in longer waiting time for the packets to be processed by the application layerin each OBU.

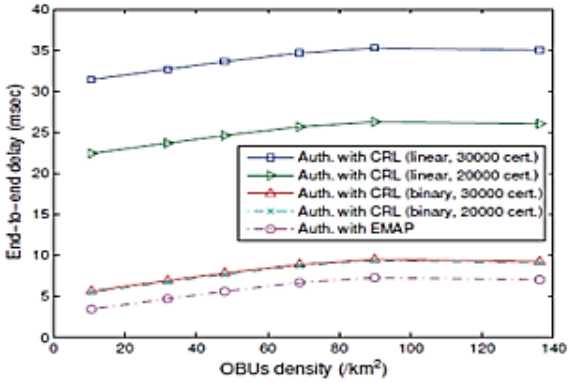

Fig. 3 End to end delay vs OBU Density

It can be seen that the end-to-end delay increases with the OBUs density because the number of the received packetsincreases with the OBUs density resulting in longer waiting time for the packets to be processed by the application layerin each OBU.

IV. CONCLUSION

We've proposed EMAP for VANETs, which expedites message authentication by changing the time-ingestingCRL checking procedure with a rapid revocation checking approach employing HMAC function. The proposed EMAP makes use of anovel key sharing mechanism which enables an OBU to replace its compromised keys although it earlier neglected somerevocation messages. Moreover, EMAP has a modular feature rendering it integrable with any PKI method.Moreover, it is immune to normal attacks whilst outperforming the authentication tactics using thetraditional CRL. Therefore, EMAP can vastly lessen the message loss ratio because of message verification extendin comparison with the conventional authentication methods using CRL checking.

REFERENCES

[1] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communicationsystems: a position paper," Proc. Workshop on Standards for Privacy in User-Centric Identity Management, Zurich,Switzerland, July 2006

[2] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacyfor VANET," Proc. Embedded Security in Cars (ESCAR), November 2005.

[3] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed certificate service scheme for vehicular networks," IEEETrans. on Vehicular Technology, vol. 59, pp. 533–549, 2010.

[4] M. Raya and J.-P.Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68,2007.

[5] "US bureau of transit statistics." [Online]. Available: http://en.wikipedia.org/wiki/Passenger vehicles in the United States

[6] J. J. Haas, Y. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism forVANET," Proc. 6th ACM international workshop on VehiculArInterNETworking, pp. 89–98, 2009.

[7] "IEEE trial-use standard for wireless access in vehicular environments - security services for applications and managementmessages," IEEE Std 1609.2-2006, 2006.

[8] "5.9 GHz DSRC." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[9] A. Wasef and X. Shen, "MAAC: Message authentication acceleration protocol for vehicular ad hoc networks," Proc. IEEEGLOBECOM'09, 2009.

[10] J. P. Hubaux, "The security and privacy of smart vehicles," IEEE Security and Privacy, vol. 2, pp. 49–55, 2004.

[11] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs,"Proc. SECON '09, pp. 1–9, 2009.

[12] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P.Hubaux, "Eviction of misbehaving and faulty nodes in vehicularnetworks," IEEE Journal on Selected Areas in Communications, vol. 25, pp. 1557–1568, 2007.

[13] P. P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate revocation list distribution in vehicular communicationsystems," Proc. 5th ACM international workshop on VehiculAr Inter-NETworking, pp. 86–87, 2008.

[14] K. P. Laberteaux, J. J. Haas, and Y. Hu, "Security certificate revocation list distribution for VANET," Proc. 5th ACMinternational workshop on VehiculAr Inter-NETworking, pp. 88–89, 2008.

[15] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," Proc. 2003 IEEE Symposiumon Security and Privacy, pp. 197–213, 2003.

Authors:

Divya Boya Completed M.Tech (SE) and working as Asst. Professor in Arjun College of Technology and Science.

Sravya Boya Completed M.Tech (SE) and working as Asst. Professor in Arjun College of Technology and Science.