ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 116-121 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

EMAP: A Novel Approach for Providing the Security in the Vehicular Ad Hoc Network (VANET)

[1]S.Durga Bhavani, [2] Dr. P. Harini
[1]Final M Tech Student, [2]Professor & HOD
[1,2]Dept of Computer Science and Engineering,
[1,2]St. Ann's College of Engineering & Technology, Chirala, Prakasam.dt, A.P.

ABSTRACT:A vehicular ad hoc network (VANET) utilizes cars as mobile nodes in a MANET to generate a mobile network. In the vehicular ad hoc networks the protection is an important concern. For protection, Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs). In the Public Key communications system, the authentication of a received message is perform by scrutiny if the certificate of the sender is included in the current Certificate Revocation Lists(CRLs) and verifying the authenticity of the certificate and signature of the sender. But it takes additional time for CRL checking process. So, in order to avoid this problem we use an efficient revocation check process in EMAP uses a keyed Hash Message Authentication Code(HMAC) , where the key used in manipulating the HMAC is shared only among non-revoked On-Board Units (OBUs). In addition, EMAP utilizes a new probabilistic key distribution, which allows non-revoked OBUs to securely share and update a secret key. By using this method we significantly decrease the message loss ratio. But in this method generating and verifying such signatures can origin high computational overhead. So, to overcome this trouble we introduce an new technique called ASIA as an Accelerated Secure In-network Aggregation plan that can accelerate message verifications and extensively reduce computational overhead while preserving reasonable security. ASIA can largely accelerate message verifications and significantly reduce computational and communication overhead compared to existing method.

KEYWORDS: Hash Message Authentication Code, Expedite Message Authentication Protocol (EMAP), Certificate Revocation Lists (CRLs).

I. INTRODUCTION

A vehicular ad hoc network (VANET) utilizes cars as mobile nodes in a MANET to generate a mobile network.[1] A VANET turns every contributing car into a wireless router or node, allowing cars roughly 100 to 300 meters of each other to connect and, in turn, generate a network with a wide range. 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 expected that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for protection purposes.

Vehicular communication systems are a type of network in which vehicles and roadside units are the communicating nodes, provided that each other with information, such as safety warnings and traffic information. As a supportive approach, vehicular communication systems can be most effective in avoiding accidents and traffic congestions than if every vehicle tries to solve these problems individually. Normally, vehicular networks are considered to contain two types of nodes: vehicles and roadside stations. Both are dedicated short-range communications (DSRC) devices.

Secure communication

When two things are communicating and do not want a third party to listen in. For that they need to communicate in a way not vulnerable to eavesdropping or interception.[1][2] Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot stop what was said. Other than spoken face-to-face communication with no possible eavesdropper, it is probably safe to say that no communication is assured secure in this sense, though practical obstacles such as legislation, resources, technical issues (interception and encryption), and the absolute volume of communication serve to limit surveillance.

With several communications taking place over lengthy distance and mediated by technology, and increasing responsiveness of the significance of interception issues, technology and its compromise are at the heart of this debate. For this cause, this article concentrated on communications mediated or intercepted by technology.

Message Authentication

Message authentication allows one party—the sender—to send a message to another party—the receiver—in such a way that if the message is modified en 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 seemed acceptable is arriving in the same condition that it was sent out—with no bits inserted, missing, or modified.

The goal of message authentication is for two parties (say, Alice and Bob) who share a secret key to ensure the integrity and authenticity of the messages they exchange.

A C**ertificate Revocation list** (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted.

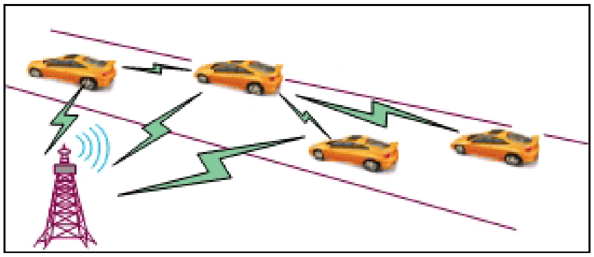
Technology:

Intelligent vehicular ad-hoc network (InVANET) is another term for promoting vehicular networking. InVANET integrates multiple networking technologies such as Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA and ZigBee.

Vehicular adhoc networks are expected to implement wireless technologies such as dedicated short-range communications (DSRC) which is a type of Wi-Fi. Other candidate wireless technologies are cellular, satellite, and WiMAX. Vehicular ad hoc networks can be viewed as component of the intelligent transportation systems (ITS).

As promoted in ITS, vehicles communicate with each other via inter-vehicle communication (IVC) as well as with roadside base stations via roadside-to-vehicle communication (RVC).

Vehicular Ad-Hoc Networks (VANET) are becoming an integral technology for connecting daily life to computer networks. They could greatly improve the driving experience both in terms of safety and efficiency. As shown in Figure 1, when multi-hop communication is implemented, VANET enables a vehicle to communicate with other vehicles which are out of sight or even out of radio transmission range. It also enables vehicles to communicate with roadside infrastructure. VANET will likely be an essential part of future Intelligent Transportation Systems (ITS).



Figure(1). Vehicle Ad-Hoc Networks

VANET can also serve as a large-scale wireless sensor network for future ITS because every modern vehicle can be regarded as a super sensor node.

II. RELATED WORK

P. Papadimitratos stated that the emerging technology of vehicular communications (VC) raises a number of technical problems that needto be addressed. Among those, security and privacy concernsare paramount for the wide adoption of VC. In this positionpaper, we are concerned with privacy and identity managementin the context of these systems. We identify VC-specific issues andchallenges, considering the salient features of these systems. Inparticular, we view them in the context of other broader privacyprotection efforts, as well as in the light of on-going work forVC standardization, and other mobile wireless communicationtechnologies.

Krishna Sampigethaya, LepingHuangy, Mingyan Li, RadhaPoovendran¤, KantaMatsuuray, Kaoru Sezakiy.Stated that In vehicular ad hoc networks (VANET), it is possibleto locate and track a vehicle based on its transmissions, duringcommunication with other vehicles or the road-side infrastructure.This type of tracking leads to threats on the location privacyof the vehicle's user. In this paper, we study the problem ofproviding location privacy in VANET by allowing vehicles toprevent tracking of their broadcast communications. We first, identify the unique characteristics of VANET that must beconsidered when designing suitable location privacy solutions.Based on these observations, we propose a location privacyscheme called CARAVAN, and evaluate the privacy enhancementachieved under some existing standard constraints of VANETapplications, and in the presence of a global adversary.

Wasef, A. stated that Vehicular ad hoc networks (VANETs) adopt the public key infrastructure (PKI) and certificate revocation lists (CRLs) to reliably secure the network. In any PKI system, the authentication of a received message is performed by checking that the certificate of the sender is not included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. In this paper, we propose a message authentication acceleration (MAAC) protocol for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation check process. The revocation check process uses a keyed hash message authentication code (HMAC), where the key used in calculating the HMAC is shared only between non-revoked on-board units (OBUs). In addition, the MAAC protocol uses a novel probabilistic key distribution, which enables non-revoked OBUs to securely share and update a secret key. By conducting security analysis and performance evaluation, the MAAC protocol is demonstrated to be secure and efficient.

III. EXISTING SYSTEM

In the existing system, an expedite message authentication protocol is used to provide security in vehicular adhoc networks. To ensure reliable operation of vehicular adhoc networks(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. The ability to check a Certificate Revocation Lists (CRL) for a large number of certificates in a timely manner leads an inevitable challenge to vehicular adhoc networks. Most of the existing works overlooked the authentication delay resulting from checking the Certificate Revocation Lists (CRL) for each received certificate. We propose an Expedite Message Authentication Protocol (EMAP) to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL. EMAP is suitable not only for VANETs but also for any network employing a PKI system. To the best of our knowledge, this is the first solution to reduce the authentication delay resulting from checking the CRL in VANETs. 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 shared only between unrevoked OBUs. In addition, EMAP is free from the false positive property which is common for lookup hash tables. Therefore, EMAP can significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking.

Disadvantages of existing system:

- ➢ High Computation overhead
- ➢ Not efficient

IV. PROPOSED SYSTEM

In order to reduce the computation overhead in the secure vehicular adhoc networks we introduce an innovative technique called ASIA as an effective and efficient scheme for securing data aggregation in VANETs. This approach can dramatically accelerate message verification because it mainly relies on hash operations which are several orders of magnitude faster than the digital signature scheme. It is able to largely reduce both communication and computational overhead compared to previous strategies. ASIA consists of two basic security mechanisms: Aggregate Consistency Check (ACC) and Generation-Skipping Verification (GSV). Our idea in designing ACC is providing security through introducing redundancy into the aggregation data flow. To this end, we use a directed acyclic graph (DAG) as the aggregation structure instead of the commonly used tree graph. When performing aggregation in a DAG, one node sends its messages to multiple upstream nodes. Messages with identical content flow through network and will reach eventually a common node which can compare the received messages to detect potential misbehavior during the aggregation process. The main contributions of this work are listed below:

- ✓ We propose two novel security mechanisms for data aggregation in VANETs, which are resource-conserving in terms of both computation and communication, and enable timely message verification
- ✓ We describe a complete aggregation framework from the construction of aggregation structure to the actual data aggregation phase and provide security mechanisms throughout various stages.
- ✓

Advantages of Proposed System:

- ➢ Less computation and communication overhead
- ➢ More efficient

In the proposed system HMAC code is used as OBUscan communicate with each without the interventionof the TA. In the EMAP when an OBU receives amessage, it sends the sender's id to RSU which in turnto TA. TA will check in the CRL for the revokedcertificates to check whether the OBU is revoked ornot and only after this long checking process thecommunication takes place. To reduce the time delaycaused during this authentication process we useHMAC code. If an OBU wants to communicate withother OBU, it sends an encrypted message with aHMAC code generated using the HMAC algorithmwhich will be generated by using the sender id andcommon secret key which knows all the unrevokedOBUs. The receiver OBU also generates the HMACcode by using common secret key. If the HMAC codeis same, it means that the receiver node understandsthat the sender OBU is an authenticated one.Otherwise it would not process the message.

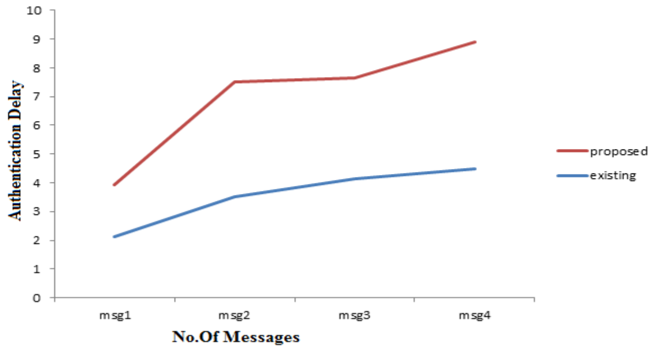
For preserving privacy, OBU does not sign andencrypt the shared secret between itself and therequesting vehicle. To sign a message, a vehiclegenerates a pseudo identity and the correspondingsigning key.

In the revocation process, each OBU have thecommon secret key which is shared between all thelegitimate OBUs. Also, each OBU is pre-loaded witha set of asymmetric keys RS and RP .Those keys arenecessary for generating and maintaining a commonshared secret key between unrevoked OBUs. Therevocation is triggered by the TA when there is anOBU to be revoked. The certificates of OBU must berevoked. In addition, the secret key set of OBU andthe current secret key Kg are considered revoked.Hence, a new secret key K˜g should be securelydistributed to all the non-revoked OBUs. Also, eachnon-revoked OBU should securely update thecompromised keys in its key sets RS and RP.

Pseudo identity provides privacy. It can be traced byRSU using the Y value given by the TA whileexecuting privacy preserving algorithm. Using the Zvalue of the OBU and using its signature andpassword etc each time it can create new pseudoidentities. So with the previous pseudonym no onecan trace it. When an OBU enters under the range ofa new RSU, new shared secret key will be generatedfor Y and Z values, which prevent previous RSUsfrom revealing the OBUs privacy.

V. EXPERIMENTAL RESULTS

Our experimental results show that, it overcomes the drawbacks of existing system. the proposed system is anExpedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming CRL checking process by anefficient revocation checking process. The revocation check process in EMAP uses a keyed Hash Message Authentication Code HMAC, where the key used in calculating theHMAC is shared only between nonrevoked On-Board Units (OBUs). In addition, EMAPuses a novel probabilistic key distribution, which enables nonrevoked OBUs to securely share and update a secret key. EMAP cansignificantly decrease the message loss ratio due to the message verification delay compared with the conventional authenticationmethods employing CRL. By conducting security analysis and performance evaluation, EMAP is demonstrated to be secure and efficient.



Figure(3). Authentication Delay

The above figure differentiate the total authentication delay and the number of received messages in a Vehicular Ad Hoc Networks(VAN).

VI. CONCLUSION

We have proposed EMAP for VANETs, which expeditesmessage authentication by replacing the time-consuming CRL checking process with a fast revocation checkingprocess employing HMAC function. The proposed EMAPuses a novel key sharing mechanism which allows an OBUto update its compromised keys even if it previously missedsome revocation messages. In addition, EMAP has amodular feature rendering it integrable with any PKIsystem. Furthermore, it is resistant to common attackswhile outperforming the authentication techniques employingthe conventional CRL. Therefore, EMAP can significantlydecrease the message loss ratio due to messageverification delay compared to the conventional authenticationmethods employing CRL checking.

VII. REFERENCES

[1]. Vehicular Ad-Hoc Networks: An Information-Centric Perspectiveby Bo Yu, ChengzhongXu.

[2]. vehicular ad hoc network (VANET) from wikipedia.

[3]. Privacy and Identity Management for VehicularCommunication Systems: a Position Paper by P. Papadimitratos.

[4]. CARAVAN: Providing Location Privacy for VANET by Krishna Sampigethaya¤, LepingHuangy, Mingyan Li¤, RadhaPoovendran¤, KantaMatsuuray, Kaoru Sezakiy.

[5]. Securing vehicular ad hoc networks by Maxim Raya and Jean-Pierre Hubaux.

[6]. An Efficient Pseudonymous Authentication Schemewith Strong Privacy Preservation for Vehicular Communications by Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin (Sherman) Shen, Fellow.

[7]. MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks by Wasef, A.

[8]. Secure and efficient Message Authentication by using In-network Aggregation for Vehicular Ad Hoc Networks

[9]. EMAP: Expedite Message AuthenticationProtocol for Vehicular Ad Hoc Networks by Albert Wasef and Xuemin (Sherman) Shen.

AUTHORS:

Durga Bhavani Samanthula received the B.Tech degree in Computer Science & Engineering from JNTU Kakinada, in 2011 & pursuing her M.Tech in Computer Science & Engineering from JNTU Kakinada.

Dr. P. Harini is presently working as a professor and HOD,Dept of Computer Science and Engineering, in St.Ann's College of Engineering and Technology, Chirala.She obtained PhD in distributed and Mobile Computing from JNTUA, Ananthapur. She Guided Many UG and PG Students. She has More than 18 Years of Excellence in Teaching and 2 Years of Industry Experience. She published more than 20 International Journals and 25 Research Oriented Papers in Various Areas. She was awarded **Certificate of Merit** by JNTUK, Kakinada on the University Formation Day on 21 - August - 2012.