Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 8, August 2013, pg.70 – 75

RESEARCH ARTICLE

AIM OF PROTECTED ROUTING MESSAGE AUTHENTICATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS

R. UmaSaraswathi[1], N. Kavitha[2], G. KesavaRaj[3]

[1]Research Scholar, Department of Computer science, Vivekanandha College, Elayampalayam, Tiruchengode-637205, India

[2]Research Scholar, Department of Computer science, Vivekanandha College, Elayampalayam, Tiruchengode-637205, India

[3]Assistant Professor, Department of Computer Application, Vivekanandha College, Elayampalayam, Tiruchengode-637205, India

[1] umaraj.tg@gmail.com; [2] msckavithan@gmail.com; [3] kesavaraj@gmail.com

Abstract— Vehicular ad hoc networks (VANETs) recognize the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their safety. In some PKI system, the certification of a predictable message is performed by examination if the certificate of the sender is included in the current CRL, and verifying the genuineness of the certificate and signature of the sender. In this paper, we recommend an Aim of protected Routing Message Protocol for VANETs, which replaces the lengthy CRL examination route by an efficient revocation checking process. The revocation check process in PRMAC uses a keyed Hash Message Authentication Code ð PRMAC, where the key used in calculating the PRMAC is shared only between non revoked On-Board Units (OBUs). In addition, PRMAC uses a novel probabilistic key delivery, which enables non revoked OBUs to securely share and update a secret key. PRMAC can extensively reduce the message loss ratio due to the message verification delay compare with the traditional authentication method employing CRL. By perform security analysis and presentation evaluation, PRMAC is confirmed to be protected and resourceful.

Key Terms: - Certificate Revocation; Communication Security; Hash Message; Message Authentication; Vehicular Networks

I. INTRODUCTION

The Vehicular Ad Hoc Network (VANET) has received considerable attention in current years, and the related principles and applications [1][2] are promote in many countries. The VANET provides both Roadside-to-Vehicle Communication (RVC) and Inter-Vehicle Communication (IVC). VEHICULAR ad hoc networks (VANETs) have scared broad kindness newly as a promise technology for change the transportation systems and providing broadband communication services to vehicles. VANETs consist of entities including On-Board Units (OBUs) and transportation Road-Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) infrastructure are the two basic communication modes, which, respectively, allow OBUs to communicate with each other rand with the infrastructure RSUs.

Since vehicles communicate through wireless channels, a Variety of attacks such as injecting false information, Modifying and replaying the spread messages can be easily launched. A security attack on VANETs can have severe harmful or fatal penalty to legitimate users. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. A well-recognized resolution 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 a genuine certificate, and every message should be digitally signed previous to its communication.

A CRL, usually issued by a Trusted Authority (TA), is lists contain all the revoked certificates. In a PKI system, the support of any message is performed by first checking if the sender's certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender's certificate, and finally verifying the sender's signature on the received message. The first division of the endorsement, which checks the revocation rank of the sender in a CRL, may incur long delay depending on the CRL size and the employed instrument 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, i.e., to abstain the escape of the real identities and location information of the drivers from any exterior eavesdropper [1], [2], [3], each OBU should be preloaded with a set of unsigned digital certificates, where the OBU has to periodically change its anonymous certificate to mislead attackers [4], [5], [6]. Consequently, a revocation of an OBU results in revoking all the certificates carried by that OBU leading to a large increase in the CRL size.

2) The scale of VANET is very large. According to the United States Bureau of Transit Statistics, since the number of the OBUs is huge and each OBU has a set of certificate, the CRL size will enlarge radically if only a small portion of the OBUs is revoked.

To have an idea of how large the CRL size can be, consider the case where only160 OBUs are revoked, and each OBU has 26,000 certificates [8]. In this case, the CRL contains 2.6 million revoked certificates. According to the employed system for searching a CRL, the Wireless Access in Vehicular Environments normal does not state that either a non-optimized search algorithm, e.g., linear search, or some sort of optimized search algorithm such as binary search, will be used for searching a CRL. According to the Dedicated Short Range Communication (DSRC) [10], which is part of the WAVE standard, each OBU has to broadcast a message every 300 m/sec about its location, velocity, and other telemetric information. In such scenario, each OBU may receive a large number of messages every 300 m/sec, 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 inevitable challenge to VANETs. To ensure reliable 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. Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received Certificate. In this paper, we introduce protected Routing Message Authentication Protocol (PCMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and protected PCMAP function. PCMAP 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.

II. RELATED WORK

Vehicular ad hoc networks (VANET) are a new technology that has recently drawn the attention of the industry and academia. Vehicular communications (VC) lie at the core of a number of research initiatives that aim to enhance safety and efficiency of transportation systems; with envisioned applications providing, for example, warnings on environmental hazards (e.g., ice on the pavement), traffic and road conditions (e.g., emergency braking, congestion, or construction sites), and local (e.g., tourist) information. In fact, vehicular networks emerge, among civilian communication systems, as one of the most convincing and yet most challenging instantiations of the mobile ad hoc networking technology. To enable such applications, vehicles and road-side infrastructure units (RSUs), namely network nodes, will be equipped with on-board processing and wireless communication modules.

Then, vehicle-to-vehicle (V2V) and vehicle- to-infrastructure (V2I) (bidirectional) communication will be possible directly when in range, or, in general, across multiple wireless links (hops), with nodes acting both as end points and routers. Relying on such hybrid networking appears to be the only means to realize safety and driving assistance applications, as an omnipresent infrastructure can be impractical, too costly, and thus very slowly deployed. A comprehensive set of security mechanisms integrated into the VC systems is critical for their deployment. Otherwise, the efficiency of the transportation systems, as well as the physical safety of

vehicles, drivers, and passengers could be jeopardized. Even worse, VC-based applications can be of life critical nature. At the same time, VANETs are particularly challenging to secure due to the tight coupling between applications and the networking fabric, as well as additional societal, legal, and economical considerations, which raise a unique combination of operational and security requirements.

A small number of recent works are concerned with different aspects of security and privacy of vehicular networks, either outlining challenges [1], [3], describing particular attacks [4], [5] or more general attack overviews [1], offering general suggestions towards solutions [15], [9], or proposing mechanisms [6], [7], [5], [8]. Nevertheless, the literature provides neither a coherent view of the VC systems, with respect to their characteristics and the security and privacy requirements, nor a roadmap towards mechanisms that satisfy them. In this paper, we seek to bridge this gap and provide a solid basis for the development of future vehicular security schemes. As VC is a technology in the making, our investigation draws from the current understanding and projections from both the academic and industry worlds. At the same time, we point out the unique or novel aspects due to VC salient characteristics. We first provide a concise problem statement and motivation and then list general security requirements. Schemes satisfying these requirements could be viewed as building blocks for any possible solution. Then we compile a set of operational characteristics and provide a minimal set of assumptions on the system and the communication model. Then, we investigate models of benign failures and models of adversarial behavior, and discuss the suitability of existing adversary models for the VC environment. Then we propose a set of design principles for any security solution for vehicular networks to follow. We conclude with a discussion on additional aspects and connections to practical considerations.

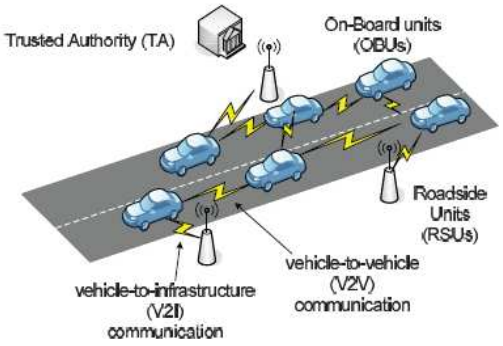

Fig. 2. The system model.

Fig. 1 The System Model

III. PRELIMINARIES

In this section, we introduce the bilinear pairing, hash chains, and search algorithms that can be employed for checking a CRL.

A. Bilinear pairing

The bilinear pairing is one of the foundations of the proposed protocol. Let GG1 denote an additive group of prime order q, and GG2 a multiplicative group of the same order. Let P be a generator of G1, and ê: -> G1 X G1 G2 is a bilinear mapping with the following properties:

1. Bilinear ê (aP; bQ) = ê (P; $Q^{)ab}$, for all P, Q € G1 and a; b $€_R$ Zq.
2. No degeneracy: ê (P; Q) $\neq 1_{G2}$.
3. Symmetric: ê(P;Q) = ê (Q; P), for all P;Q € G1.
4. Admissible: the map ê is efficiently computable.

The bilinear map ê can be implemented using the Weil and Tate pairings on elliptic curves.
The security of the proposed protocol depends on solving the following hard computational problem:

Elliptic curve discrete logarithm problem (ECDLP). Given a point P of order q on an elliptic curve, and a point Q on the same curve. The ECDLP problem is to determine the integer l, $0 \leq l \leq q - 1$, such that Q = lP.

B. Hash Chains

A hash chain is the successive application of a hash function h: {0; 1}* -> Z * with a secret value as its input. A hash function is easy and efficient to compute, but it is computationally infeasible to invert.

C. Search Algorithms

The WAVE standard does not consider a specific mechanism for searching CRLs to check the revocation status of certificates. The most common search algorithms include no optimized search algorithms such as linear search algorithm, and optimized search algorithms such as binary search algorithm and lookup hash tables. The basic concept of each algorithm is as follows: Linear Search Algorithm In the linear search algorithm, the revocation status of a certificate is checked by comparing the certificate with each entry in the CRL. If a match occurs, the certificate is revoked and vice versa.

1) Binary Search Algorithm: The binary search algorithm works only on sorted lists. Consequently, upon receiving a new CRL, each OBU has to maintain a sorted (with respect to the certificate's identity) database of the revoked certificates included in previous CRLs and the recently received CRL. The main idea of the binary search algorithm is to cancel out half of the entries under consideration after each comparison in the search process. In the binary search, the revocation status of a certificate is checked by comparing the identity of the certificate with middle value (which in this case will be the median value) of the sorted database. If the identity of the certificate is greater than the median value, the right half of the database will be considered in the next comparison process and vice versa. This process continues until a match is found, i.e., the certificate is revoked, or the process is finished without finding a match which means that the certificate is unrevoked.

2) Lookup Hash Tables: In this approach, the set of all possible certificates (U) is mapped using a hash function into a table of n entries. To check the revocation status of a certificate, the hash of the certificate's identity is the index of the entry in the lookup table which should be checked to determine the revocation status of the certificate. If nil is found in that entry, the certificate under consideration is unrevoked and vice versa. Since VANETs scale is very large and each OBU has a set of certificates, the size of U will be huge compared to the size (U) of the lookup table. Consequently, the probability of hash collisions will be high, which directly translates to a high probability of false positives.

Here, a false positive means that the certificate of an innocent OBU is falsely considered revoked which results in rejecting all the messages containing the certificate of that OBU. The rejected messages may include a warning from dangerous situations. Hence, rejecting these messages may deprive the recipient OBU from taking the appropriate countermeasures to ensure its safety. Accordingly, lookup hash tables may not be practical for VANETs. Hence, lookup hash tables will not be considered in this paper. It should be noted that hash functions which map an input to one entry of possible n entries used in the lookup tables, are different from cryptographic hash functions which map an input to a unique output. Throughout the rest of the paper, the considered hash functions are cryptographic hash functions.

IV. PROTECTED ROUTING MESSAGE AUTHENTICATION PROTOCOL

The proposed PMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution. Our OLSV protocol is sub-divided into three parts, namely sender, receiver, and recovery. Every router runs a sender process, a receiver process, and a recovery process. The sender process generates keys and uses them to generate MAC for LSU. Those LSU and the associated MACare then flooded to other routers as in existing link state routing protocols. The keys are released to other routers at designated times. The receiver process optimistically accepts LSU (as if they were authenticated) and uses them to compute the local routing table.

When the corresponding keys arrive, the receiver process verifies the authenticity of the LSU received. When the receiver process detects mischievous LSU, the recovery process is invoked. A recovery process is responsible for diagnosis and reconfiguration. Diagnosis is used to locate misbehaving routers. Based on the diagnosis results, reconfiguration is used to logically disconnect that misbehaving routers from the network to restore its operational status. The recovery process is designed to counter router attacks. To counter active link attacks, neighboring routers use a MAC scheme to authenticate LSU forwarded between them. Because a router usually has few neighbors, a secret key can be configured or established using a key-exchange protocol for each neighboring router pair and many existing efficient MAC schemes are applicable to authenticate LSU sent between neighboring routers. For the sake of clarity, we omit this LSU authentication between neighboring routers in the subsequent description of our protocol.

A. Sender Process

The sender process generates a random quantity r and Constructs a hash chain of length ` using r and a one-way hash function H. Subsequently, the sender process composes a key-chain anchor (KCA) message that contains the router id, the current time T, and $H^{l}(r)$ and signs it with the private key of the router. Then the signed KCA message (id, T, Ht(r), Sid (id, T, Ht(r)) is distributed to other routers via flooding.

The quantities $H^{i-i}(r)$, where $1 \leq i \leq 1$ `, are used as keys to generate MAC for LSU. A hash-chained key (HCK) message (id; i; $Hl^{-i}(r)$) is released to other routers at time T +I D, where D is the duration of the time intervals between consecutive key releases. In fact, the sender process only needs to release a HCK if the corresponding $H^{l-i}(r)$ is used to generate a MAC. To make OLSV secure, $H^{l-i}(r)$ is used to generate MAC for LSU only before time T +iΔ, where T is a value that we will derive later.

B. Receiver Process

When the receiver process receives a KCA with a digital S_{id} (id, T, H (r)) signature Sid(id; T;H`(r)), it verifies the authenticity of the KCA using the public key of outer id. A verified KCA with T reasonably close to the current clock value of the router is accepted and stored.

The receiver process optimistically accepts a signed LSU (LSU, i, MACGHe-1(r) (LSU,i)) i)) if the receiving time is less than T +i + iD-€ (Note that the router id in LSU can be used to determine the corresponding). When a HCK message (id, i, k)) is received, the authenticity of the HCK is verified by applying the hash function.

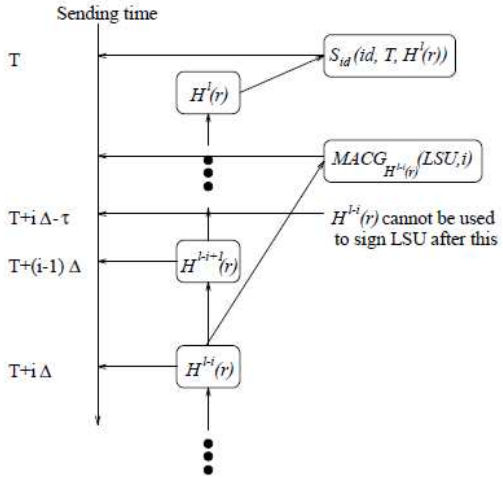

Fig.2 The Sender Process

V. CONCLUSIONS

We have future PRMAC for VANETs, which expedites announcement authentication by replace the slow CRL checking process with a fast revocation checking development employ HMAC function. The proposed PMAP uses an original key allocation means which allows an OBU to renew its compromise key even if it in the past missed some revocation messages. In toting up, PMAP has a modular feature rendering it integral with any PKI system. Furthermore, it is resistant to common attacks while outperforming the authentication techniques employs the conformist CRL. Therefore, PMAP can considerably decrease the memo loss ratio due to message verification wildcat strike compare to the straight proof methods employing CRL checking. Our future work will focus on the certificate and message name corroboration acceleration.

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] 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] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications, IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.
[6] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets, IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.
[7] US Bureau of Transit Statistics, http://en.wikipedia.org/wiki/Passenger_vehicles_in_the_United_States, 2012.
[8] 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 Vehicule Ar Inter NET working, pp. 89-98,2009.
[9] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.
[10] 5.9 GHz DSRC, http://grouper.ieee.org/groups/scc32/dsrc/index.html, 2012.
[11] Wasef and X. Shen, MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks, Proc. IEEE GlobeCom, 2009.
[12] J.P. Hubaux, The Security and Privacy of Smart Vehicles, IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.
[13] 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.
[14] 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.
[15] 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.
[16] 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.

