BRAT : AN EFFICIENT SIGNATURE SCHEME FOR VEHICULAR NETWORKS USING BINARY RE-AUTHENTICATION TREE

Suganya[1], K. Ravikumar[2]

ABSTRACT

In this paper, It propose Binary Re-Authentication tree a relatively efficient signature scheme for vehicle – to – infrastructure communication. The BRAT Scheme can use Secure Hash Algorithm (SHA) algorithm can efficiently eliminate the performance bottleneck when verifying a mass of signatures with other verifying a mass of signatures with other ECDCA algorithm for the solution of bogus messages and DOS – tolerant signature scheme. In addition, Zero Knowledge Protocol (ZKP) to address this problem of re-authentication and achieves Re authentication by neighborhood authentication of the node that wants to rejoin the network. In addition it attempts to identify the possible future direction for this field. It also discusses the implementation details of these systems including the phases by them and the metrics are used to measure the performance. It offers the other conventional security for vehicular networks, such as privacy identification and traceability.

Keywords : *BRAT, ZRP, SHA, Vehicular Communication, signatures, BAT, ECDCA.*

[1]Research Scholar, Department of Computer Science, Karpagam University, E-mail: mailtosuha@gmail.com

[2]Research Scholar, UGC NET-Co-Ordinator, Department of Computer Science,
Tamil University. E-mail: ravikasi2001@gmail.com

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are the two basic communication modes, which respectively, allow OBUs to communicate with each other and with the infrastructure RSUs. Vehicular communication over the wireless medium employs the Dedicated Short Range Communications (DSRC) protocol [1].

A vehicular network needs strong authentication, because it is desirable to Validate each message sent by the On Board Units (OBUs). It is recognized solution is to sign each message with a signature [2][3]. However, classic signature schemes that sequentially verify the messages may fail to satisfy the real-time requirement in vehicular communications. According to DSRC protocol [1], a RSU may communicate with hundreds of OBUs and each OBU will periodically transmit a safety or traffic message (beacon) to the nearest RSU via a common DSRC channel. Recently, an efficient batch verification scheme for optimizing the verification performance in V2I

communications without any bogus messages has been proposed [4]. A prerequisite condition in this method is that all the signatures should be authentic.

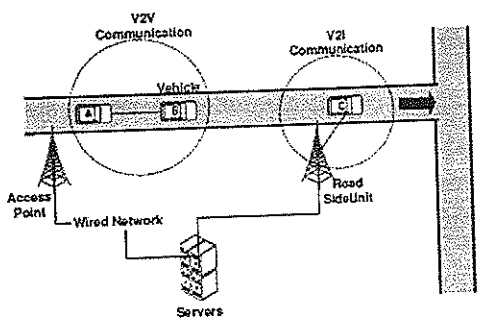

Figure 1 : Illustration of inter-vehicle communication and the components involved. The circles indicate communication better the enclosed nodes.

Fig. 1 illustrates a typical VANET that consists of vehicles, access points on road side, and a collection of location servers. Vehicles move on roads, sharing collective environmental information be taken themselves, and with the servers via access points. DSRC is under active development in the United States and in other countries. The goal of the paper is to explain the content and status of the major standards that support interoperable DSRC in the United States [5][6].The primary motivation for deploying DSRC is to enable collision prevention applications. These applications depend on frequent data exchanges among vehicles, and betIten vehicles and roadside infrastructure.

II. Related Work

The IEEE 802.11p task group is working on the Dedicated Short Range Communications (DSRC) Standard, which aims to enhance the 802.11 protocol to support wireless data communications for vehicles and roadside infrastructure [4].The Vehicle Safety Communications Project was to evaluate the feasibility of using the DSRC Standard to support the roadside safety related applications [7]. In [8], a solution was proposed to take advantage of a list of short-lived anonymous certificates to keep the privacy of the drivers, where the short lived certificates are discarded right after being used.

Raya et al. [14] also propose a PKI-based security and privacy protocol, where each vehicle needs to pre-load a huge pool of anonymous public/private keys, and the trusted authority also needs to store all the anonymous certificates of all the vehicles, which incurs inefficiency for certificate management. In [15], an approach to implement privacy in VANETs is presented by using geo-bounded pseudonyms and a trusted third party. Another PKI-based architecture for authentication and authorization is proposed using the Kerberos model by Moustafa et al. [6].

III. Preliminaries

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

A. Bilinear Pairing

The bilinear pairing [8] 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 GG1, and GG1 _ GG1 ! GG2 be a bilinear mapping with the following properties:

1) Bilinearity: □ Q,R, S □ $G1$ and a, b □ Z, $e(R,Q+S) = e(Q + S,R) = e(Q,R)e(S,R)$.

2) Non-degeneracy: □Q,R □ $G1$ such that $e(Q,R) =1G2$.

3) Computability: □Q,R □ $G1$, there is an efficient algorithm to calculate $e(Q,R)$.

Such a bilinear map e can be constructed by the modified Itil [13] or Tate pairings [14] on elliptic curves. A group with such a map e is called a bilinear group, 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 [23] is to determine the integer l, 0 < l< q< 1, such that Q ¼ lP .

B. Application Scenario Model

As shown in Fig. 2, It consider the representative Vehicle-to-Infrastructure communications architecture, which includes:

1) **RSU**: A RSU serves as a gateway connecting the vehicles within its transmission range to the Internet.

2) **Vehicles**: A vehicle periodically exchanges messages with the RSU within its range. Each vehicle is equipped with sensing and processing units, OBUs (On-Board Units).

3) **TA** (Trusted Authority): The TA server, as the key distribution center, is responsible for generating and assigning related parameters for the vehicles and RSUs,and identifying a malicious identity for any dispute events.

4) **SP** (Service Provider): The SP or Application Server is responsible for collecting the traffic related information such as location, traffic accidents, and other important information from RSUs, and making further analysis and giving response to RSUs.

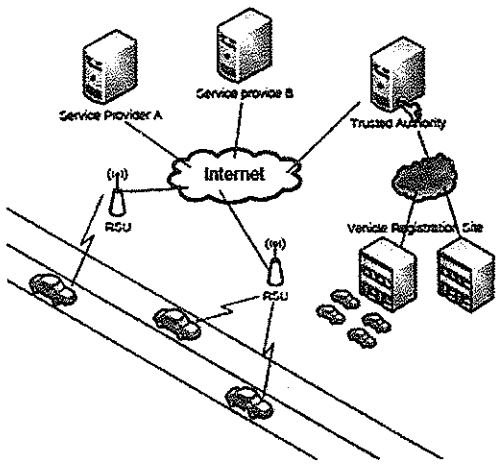

Figure 2 : Application Scenario Model

5) **VRS** (Vehicle Registration Site).

A RSU may communicate with hundreds of OBUs at the same time within its communication range, which relies on the DSRC broadcast protocol, the designated protocol for vehicular networks [1].

6) AS(Authentication Server) : The AS or Authentication Server is responsible for collecting the authorized user other important information from RSUs,its received only authenticated messages at the same time within communication range on DSRC.

C. Lookup Hash Tables

In this approach, the set of all possible certificates 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.

Figure 3 : Hash Chain

A hash chain [26] is the successive application of a hash function h : f{0, 1}-> $^{Z^*q}$ with a secret value as its input. A hash function is easy and efficient to compute, but it is computationally infeasible to invert.

IV. Zero Knowledge Protocol

The proposed ZRP uses a fast Hash function and novel key sharing scheme employing probabilistic random key distribution.

A. System Model

As shown in Fig. 1, the system model under consideration consists of the following:

i) A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network.

ii) Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TA.

iii) OBUs, which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications [10][11]..

According to the WAVE standard [9], each OBU is equipped with a Hardware Security Module (HSM), which is a tamper-resistant module used to store the security materials, e.g., secret keys, certificates, etc., of the OBU.

B. System Initialization

The TA initializes the system by executing Algorithm 1. In step (20), it should be noted that: PKi denotes the ith public key for OBUu, where the corresponding secret key is SKiu ;PIDi u denotes the ith pseudo identity (PID) for OBUu, where the TA is the only entity that can relate PIDi u to the real identity of OBU.

Algorithm 1.Key Generation

Key Generation (n, MAC_{Ni}, IP_{Ni}, N_{Ni}, SR_{Ni}, MP_{Ni})/ *generate MIN_i of 128 bits*/

1. Generate MIN_i a variable by appending MAC_{Ni}, IP_{Ni}, N_{Ni}. If MIN_i = 128 bits go to step 6
2. If MIN_i < 128 bits Pad '0' in the MIN_i go to step 2
3. If MIN_i > 128 bits Retaining the most significant 128 bits of MIN_i and discard the remaining bits./* acquiring server's information */
4. Acquire Server MAC Address (MAC_s), IP address (IP_s), ServerName (N_s).

5. Acquire current Date (dd/mm/yyyy), Time (hh:MM:ssss) from server when node N_i occurred.

/*generating MIN_s of 128 bits*/

6. Generate MIN_s a variable by appending MAC_s, IP_s and N_s.If MIN_s = 128 bits go to step 9

7. If MIN_s < 128 bits Pad '0' in the MIN_s go to step 7

8. If MIN_s > 128 bits Retaining the most significant 128 bits of MIN_s and discard the remaining bits.

/*generate T_i of 128 bits*/

9. Generate T_i by appending dd, mm, yyyy, hh, MM and ssss in the string Format. /* if T_i is greater than 128 bits Althen consider the most significant 128 bits and discard the rest */

/* generate random number R_i */

10. Generate 128 bits $SRMP_{Ni}$ a variable by appending 64 bits SR_{Ni} with 64 bits MP_{Ni}.

/* MP_{Ni} will be in the string format (x-coordinate appended by y-coordinate). e. g. 07400568 where x-cord= 740 and y-cord=568*/

11. R_i=$SRMP_{Ni}$ (XOR) Ti /* Here, R_i is 128 bits */

/* calculating n bits NOB variable from R_i for dynamic key generation */

12. NOB = last n-7 bits of R_i. /*(i. e. NOB=$R_{i((128-n)\ to\ 128)}$) Here, no. of bits in (NOB) = n-7 bits*/

13. append seven '0's in to the LSB side of NOB /* Here, no. of bits in (NOB) = n bits*/

14. If NOB<128 NOB=128 /* maximum value of (NOB) = (2^n-1), minimum value of (NOB) =128 where n is agreed value betIten the communicating parties. */

/* generating key K_i*/

/*MIN_{is}, $MINT_{is}$ are variables*/

15. MIN_{is} = MIN_i (XOR) MIN_s

16. $MINT_{is}$ = MIN_{is} (XOR) T_i

17. K_i = $MINT_{is}$ (XOR) R_i

/* returning Key and NOB*/

18. Key_NOB = Append(K_i, NOB)

19. Return Key_NOB

20. End

V. Security Analysis

The BRAT scheme is the same as the original scheme except the verification phase. Thus, it can also offer some conventional security properties for vehicular communications, such as identity privacy and identity traceability.

A. Identity Privacy

For any vehicle *Vi*, its real identity *IDi* is protected with the pseudo identity $PIDi = \{PIDi,k | k = 1, 2, ..., z\}$, which is computed as $PIDi,k = EKTVk\,(gvi,k = IDi)$, where $KTVk = (gvi,k)w = (gw)vi,k$.Note that each $PIDi,k$ is actually a

symmetric encryption value, which is semantic secure under chosen plaintext attacks.

Hence, for an illegal tracker with no knowledge of secret $w \in Zq$ or $vi,k \in Zq$, it is infeasible for him to derive the real identity from *PIDi*.The identity privacy is assured by two measures: 1) When vehicle *Vi* visits different RSUs, its pseudo identity *PID=i* is different due to the different *gvi,k* ; 2) there are no direct relationships among these pseudo identities *PIDi* .

B. Resistance to Replay Attacks

Since in each message an OBU includes the current time stamp in the revocation check value REV check ¼ HMAC,PID stamp, an attacker cannot record REV check at time Ti and replay it at a later time to pass the revocation checking process as the receiving OBU compares the current time Ti with that included in the revocation check. Consequently, EMAP is secure against replay attacks.

C. Message Signature

It basic signature scheme can be considered as a modified F. Hess's signature scheme [12], by replacing $Ei = \hat{e}(P, P)ri$ in Hess's scheme with $Ei = riP$.

Considering the computation capacity of a vehicle, It eliminate the complex pairing operation $Ei = \hat{e}(P, P)ri$, which is performed at the signer end in Hess's scheme. The security of It basic signature scheme also relies on the Diffie-Hellman hard problem in the random oracle model[12].

VI. Performance Evalution

It compares the BRAT scheme with both the SHA (Secure Hash Algorithm) scheme [13] and the basic scheme in terms of the verification complexity. The BRAT scheme is the signature algorithm advised by IEEE1069.2 standard [11], which is the current standard for VANETs, while the basic signature scheme was introduced in Section IV, which is the basis of the BAT signature scheme. BRAT, as a variant of the Digital Signature Algorithm (DSA), operates on elliptic curve groups.

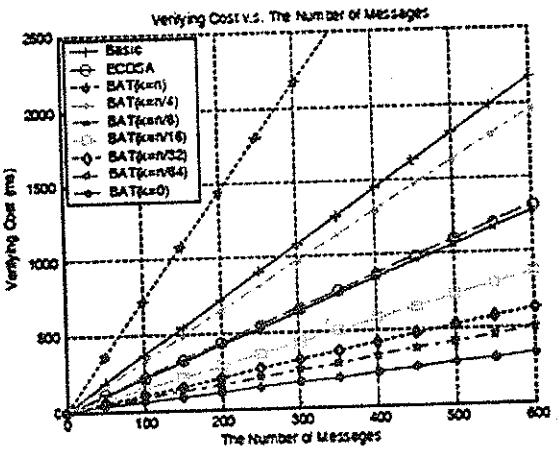

Figure 4 : Verification of Number of messages

It defines computation cost of the cryptographic operations as follows.

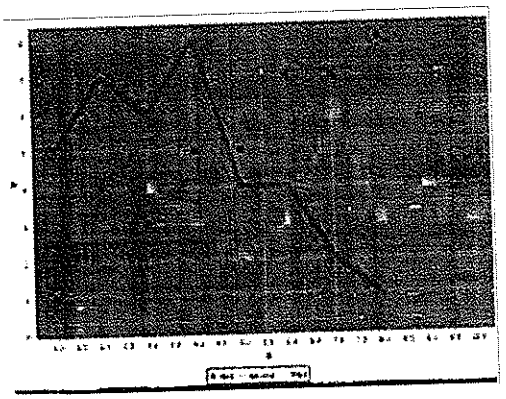

Figure 5 : Comparison Facts

VII. Conclusion

The proposed ZKP for VANETs, which Zero Knowledge Protocol authentication by replacing the time-consuming Key Generation process with a fast process employing SHA Algorithm. The proposed ZKP uses a novel key sharing mechanism which allows an OBU to update its Session keys. Making use of the Binary Re-Authentication tree model, It repair that all schemes and obtain a scheme that is provably secure and efficient. In addition, ZKP has a modular feature rendering it integrable with any PKI system. Theoretical analysis and simulation results have demonstrated that the BRAT scheme is valid and practical in efficient signature verification and meets the security and the privacy requirements for Dos-tolerant signature scheme.

Acknowledgement

It would also like to thanks the anonymous reviewers, whose comments and suggestion stimulated new thoughts helped to improve the paper.

References

[1] Dedicated Short Range Communications (DSRC), [On-line] http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[2] W. Franz, C. Wagner, C. Maihofer, and H. Hartenstein, *"Fleetnet:platform for inter-vehicle communications,"* in *Proc. 1st Intl. Workshopon Intelligent Transportation*, Hamburg, Germany, 2004.

[3] *"NoW: Network on Wheels Project,"* [On-line] http://www.network-onwheels. de, 2007.

[4] *"US Vehicle Safety Communication Consortium,"* [On-line] http://wwwnrd. nhtsa.dot.gov/pdf/nrd-CAMP3 /pages /VSCC .htm

[5] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, *" Security issues in a future vehicular network,"* in *Proc. European Wireless, Next Generation Wireless Networks*, vol. 1, pp. 270-274, 2002.

[6] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, and J.-M. Tang, *"Framework for security and privacy in automotive telematics,"* in *Proc. 2nd International Workshop on placeMobile Commerce*, pp. 25-32,2002.

[7] A. R. Beresford and F. Stajano, *"Location privacy in pervasive computing,"IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46-55, 2003.

[8] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K.Sezaki, *"CARAVAN: providing location privacy for VANET,"* in *Proc.Workshop on Embedded Security in Cars (ESCAR)*, 2005.

[9] A. Wasef and X. Shen, *"MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks,"* Proc. IEEE GlobeCom, 2009.

[10] J.P. Hubaux, *"The Security and Privacy of Smart Vehicles,"* IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.

[11] 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.

[12] 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.

[13] P.P. Papadimitratos, G. MezzIt, and J. Hubaux, *"Certificate Revocation List Distribution in Vehicular Communication Systems,"* Proc. Fifth ACM Int'l Workshop VehiculAr Inter-NETworking,pp. 86-87, 2008.

[14] Y. Jiang, M. Shi, X. Shen, and C. Lin, *"BAT: a robust signature scheme for vehicular networks using binary authentication tree"*, IEEE Transactions on Wireless Communications, vol. 8, no. 4, pp. 1974-1983, 2009.

[15] D. Boneh and M. Franklin, *"Identity-based encryption from the Itil pairing,"* in Advances in Cryptology- CRYPTO 2001, LNCS 2139, pp. 213-229, 2001.

AUTHOR'S BIOGRAPHY

Dr. K. Ravikumar working in Tamil university Thanjavur. He is Presented paper in 50 International and National Conferencesand JItnals. He is Completed UGC Research Project. He is written 16 DDE Books in Tamil University Thanjavur. He is 12 years Teaching and Research Experience. He is having UGC-NET Coaching Cocoordinator for UGC XI Plan. He is a cocoordinator for DDE cItses, Tamil University Thanjavur. His Research Areas is Network Security, Cryptography, Mobile Computing, and Cloud Computing.

Mrs. R. Suganya, working in T.U.K.Arts College, Karanthai, Thanjavur. She is presented paper in 3 International and National Conference and JItnals. She is 8 years teaching experience. Her Research area is Network Security, Cryptography and Mobile computing.