AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

CEKD: Computationally Efficient Key Distribution Scheme for Vehicular Ad-Hoc Networks

[1]M. Azees and [2]P.Vijayakumar

[1]*Research Scholar, University College of Engineering Tindivanam, Department of CSE, Tamilnadu, India.*
[2]*Dean, University College of Engineering Tindivanam, Tamilnadu, India.*

Address For Correspondence:
M. Azess, Research Scholar, Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tamilnadu, India. Tel: +91-7708976657, email: azeesmm@gmail.com

ARTICLE INFO

Article history:
Received 04 December 2015
Accepted 22 January 2016
Available online 14 February 2016

Keywords:
Group communication, Key distribution, Vehicular ad-hoc networks (VANETs), bilinear pairing, group key.

ABSTRACT

In vehicular ad-hoc networks, secure and reliable group communication is an energetic area of research. Today, the most important research challenge is an efficient group key distribution for a secure group communication. Even though there are many group key distribution protocols, they have the security and performance weakness. In this paper, we propose a computationally efficient group key distribution scheme for secure group communication based on bilinear pairing. The proposed CEKD scheme provides better performance in comparison with most of the previously proposed key distribution schemes in terms of computation cost, making it suitable for secure group communication in VANETs.

INTRODUCTION

Today, vehicle accidents are one of the leading causes of death in the world and also the traffic jams make a terrific waste of time and fuel. So the Vehicular Ad-hoc Network (VANET) has become an unavoidable subject of research to improve the driving experience, traffic safety, and multimedia infotainment propagation for VANET users. VANET can noticeably increase the knowledge of the surrounding environment of drivers in the road transport system (Zhang *et al*., 2008). Basically, a VANET consists of three major components that are vehicles or mobile nodes in which On Board Units (OBUs) are equipped for computation and communication purposes, Road Side Units (RSUs) that are fixed infrastructures located aside the roads, and a Trusted Authority (TA) has the responsibility of maintaining the whole transport system. In VANETs, a vehicle that can be shared the information with other vehicle through Vehicle-to-Vehicle (V2V) communications, or with RSU, through Vehicle-to-RSU (V2R) communications. The V2V communications and the V2R communications are used to improve traffic safety and traffic efficiency. For V2V and V2R communications, the Dedicated Short Range Communication (DSRC) radios [DSRC] are deployed in each vehicle and in all RSUs. In VANETs, RSU to TA communication and communication among RSU's are performed through a secured wired channel. But the V2V communication and the V2R communications are performed through a wireless channel. Hence, it is necessary to protect the wireless channel from the various kinds of security attacks. If the communication is not properly protected then the private data, such as the group key for group communication has to be revealed (Sun *et al*., 2010).

Several approaches have been proposed to securely distribute the group key based on the Diffie-Hellman key exchange protocol. However, the main problem with such approaches is that the man-in-the middle attack. In this attack, the intruder secretly alters the communication between two entities who believe that they are directly communicating with each other. The main purpose of the proposed key distribution scheme is to enable

To Cite This Article: M. Azees and P.Vijayakumar, CEKD: Computationally Efficient Key Distribution Scheme for Vehicular Ad-Hoc Networks. ***Aust. J. Basic & Appl. Sci.,*** *10(2): 171-175, 2016*

the TA to securely and efficiently exchange the group key to the group members in the group. The proposed scheme depends on the hardness of computing discrete logarithms.

This paper is organized as follows. Section 2 provides the related works. Section 3 presents the system model and preliminaries. Section 4 discusses the proposed CEKD scheme. Section 5 and Section 6 analyze the security strength and performance respectively. Finally, we draw the conclusion in section 7.

Related Works:

In order to distribute a group key in a secure manner, large amounts of work have been proposed. However, most of these approaches suffer from the computation overhead during key distribution. Joux (2000) proposed a tripartite key agreement protocol based on bilinear pairings over the elliptic curves. Since there is no secure authentication protocol between the communicating parties, this scheme is affected by the man-in-the-middle attack. Hao *et al*. (2008) proposed a distributed key management scheme based on group signature for a secure group communication in VANETs. In this scheme, the RSUs act as the group key distributor for each group. Since, the RSUs are considered to be semi-trusted, the compromised RSU may misbehave and reveal the group key to adversaries. Xiaozhuo *et al*. (2015) proposed a Huffman-tree-based pairing free authenticated certificateless group key agreement protocol for minimizing the group key distribution time and the rekeying time in the join/departure events. Since there is no authentication procedure between the communicating parties before the group key distribution, this scheme has a security weakness in terms of man-in-the-middle attack.

System Model and Preliminaries:

3.1 System model:

The system model of the proposed system is depicted in Fig.1. which includes a TA, fixed RSUs at the road side, and OBUs equipped in mobile vehicles.

- TA is a trusted administrative center, which provides registration to RSUs and OBUs when they join into the VANET system. The TA has the full responsibility to maintain the entire VANET system. It also divides the entire VANET system into several domains. Generally, it is assumed that the TA is infeasible to compromise by an adversary and it has high communication, computation and storage capabilities.

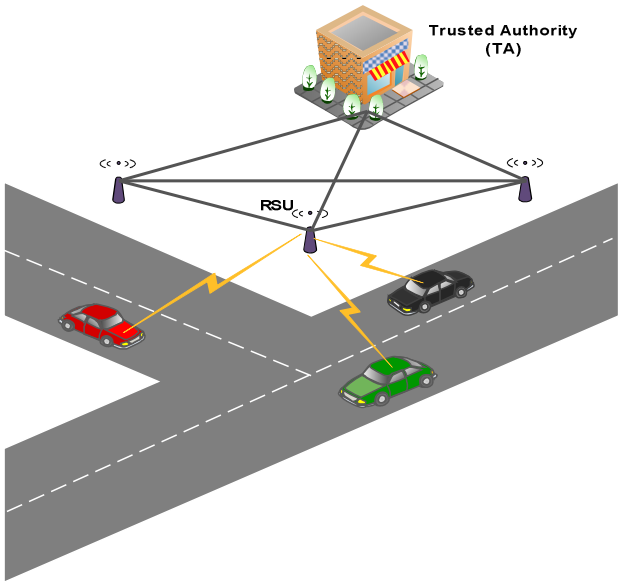

Fig. 1: System model

- RSUs communicate with vehicles in their coverage region by a wireless channel. Dedicated short range communication (DSRC) radios are implemented in both vehicles and RSUs to perform V2V and V2R wireless communications. It is assumed that RSUs are semi-trusted (Zhang, C., *et al*., 2001), i.e., they can expose secret data to adversaries, if they are compromised. In order to prevent RSUs from hardware attacks, all RSUs should be watched through hidden surveillance cameras such as digital video or analog CCTV cameras. Each RSU provides the Location Based Safety Information (LBSI) to all the authenticated vehicles when they are entered into its region. Hence, each RSU provides the knowledge to vehicle users about the obstacles within its coverage region. Table1. Shows the typical examples of some LBSIs which are broadcasted to authenticated vehicles by RSUs

Australian Journal of Basic and Applied Sciences, 10(2) Special 2016, Pages: 171-175

Table I: Location Based Safety Information (LBSI)

Information	Range
Petrol station	20 m
Speed breaker	25 m
Traffic signal	50 m
Curve speed warning	71 m
School zone	114 m
Road intersections	170 m
Accident zone	200 m

- OBUs are installed in each vehicle to communicate with other vehicles and RSUs. OBUs broadcast traffic-related status information such as location, speed, and direction periodically to other vehicles to avoid road accidents.

3.2 Bilinear Pairing:

Let G_1 and G_2 be multiplicative cyclic groups generated by P and Q respectively and G_T be a multiplicative cyclic group. G_1, G_2 and G_T have the same prime order q, i.e., $|G_1| = |G_2| = |G_T| = q$. Let $e : G_1 \times G_2 \rightarrow G_T$ is a bilinear map, which satisfies the following properties:

1) Bilinear: $e(uP, vQ) = e(P, Q)^{uv}$ for all $P \in G_1$, $Q \in G_2$ and $u, v \in Z_q^*$.

2) Nondegeneracy: There exist $P \in G_1$, $Q \in G_2$ such that $e(P, Q) \neq 1_{G_T}$.

3) Computable: Bilinear map e is efficiently computable for any $P \in G_1$, $Q \in G_2$.

Proposed CEKD Scheme:

This section has the following phases: system initialization, VANET license issuing and the proposed CEKD scheme.

4.1 System Initialization:

The TA first picks a random number $v \in Z_q^*$ as the TA's master secret key and a random number $t \in Z_q^*$ as the TA's private key. The public key of TA is computed by performing a elliptic curve based point multiplication of t with a generator P. $PU_{TA} = tP$ is the TA's public key. Then the TA publishes $\{q, PU_{TA}, P, G_1\}$ as the system parameters.

4.2 VANET license issuing:

The vehicle user first directly goes to the TA and provides their personal information (i.e., username, address, mail id, personal password, license plate number and mobile phone number) for authentication when they connect to the VANET from his/her vehicle. After providing the personal information, the TA verifies and issues the certificate CET_{V_i} to the vehicle V_i as follows.

1. TA chooses a random number $u_i \in Z_q^*$ for each vehicle and considering this as the private key of V_i, and computes its corresponding public key $PU_{V_i} = u_i P$.
2. TA then generates the VANET license VL_{V_i} for V_i, where $VL_{V_i} = vu_i P$.
3. Then, the TA computes a seed value $S = v(u_i + t)^{-1} P$ for each vehicle V_i.
4. The TA provides S, u_i, $PU_{V_i}$and VL_{V_i} to V_i in the offline mode after the successful completion of vehicle's successful registration. The values S and u_i are kept secret by the VANET user.
5. Next, TA keeps$(\mathrm{ID} - V_i, VL_{V_i}, S, u_i)$ in its tracking list, where $\mathrm{ID} - V_i$ is the identity of V_i assigned by the TA.
6.

4.3 Proposed CEKD scheme:

a. For a secure group communication, each vehicle user V_i first selects a session key $x_i \in Z_q^*$ and computes

$X_i = x_i(PU_{V_i} + PU_{TA})$

$X_i = x_i(u_i P + tP)$

$X_i = x_i(u_i + t)P$

Then, each user also computes the identification key (K_i) as follows

$K_i = e(X_i, S)$

$K_i = e(x_i(u_i + t)P, v(u_i + t)^{-1} P)$

$K_i = e(P, P)^{x_i(u_i+t)*v(u_i+t)^{-1}}$

$K_i = e(P, P)^{x_i * v}$

After computing the value of K_i, each user sends $\{X_i \parallel VL_{V_i}\}$ to the TA. After receiving these parameters from the vehicle user V_i, the TA verifies the VL_{V_i} from it's tracking list and then it computes the K_i value for each vehicle user V_i.

b. Then the TA chooses a group key $gk \in Z_q^*$ and then creates a Lagrange interpolating polynomial of degree $n-1$, where n is the number of users in the group.

$$P(y) = \sum_{i=1}^{n}(gk + u_i)\left[\prod_{\substack{j=1 \\ j\neq i}}^{n}\frac{y-K_j}{K_i-K_j}\right]$$
$$= a_0 + a_1 y^1 + \cdots + a_{n-1}y^{n-1}$$

Then the TA sends $(a_0, a_1, \ldots a_{n-1})$ to each user V_i.

c. After receiving the coefficients $(a_0, a_1, \ldots a_{n-1})$ from the TA each user V_i uses its own K_i value to recover the group key gk as follows:

$$P(K_i) = a_0 + a_1 {K_i}^1 + \cdots + a_{n-1}{K_i}^{n-1}$$
$$= gk + u_i$$

Then, each user recovers the group key by subtracting its own private key from $gk + u_i$. This group key is used to make group communication with the group members in the group.

Security analysis:

In this section, we evaluate the security strength of our proposed scheme with respect to the user authentication, impersonation attack and man-in-the-middle attack.

User Authentication:

The VANET license $VL_{V_i} = vu_iP$ for each vehicle user V_i is computed by the TA using each user's private key and its master key. So, it is assured that no other users compute VL_{V_i}except the TA who has both the private key of V_i and the master key. Since, each vehicle user V_i sends $\{X_i \parallel VL_{V_i}\}$ to the TA for getting the group key, the TA can authenticate V_i from VL_{V_i} before providing the group key to them.

Impersonation:

Let's consider that V_i's private key and its license $VL_{V_i}$is revealed. An adversary U wants to pretend as the vehicle user V_i to the TA to get the group key. However, U cannot compute the identification key K_i without knowing the seed value S which is given by the TA to V_i during the time of user registration.

Man-in-the-middle attack:

Based on the above analysis about user authentication, the proposed CEKD scheme for secure key distribution could provide authentication between the communicating parties. Therefore, the proposed CEKD scheme could withstand the man-in-the-middle attack.

Performance Analysis:

In this section, we compare the performance of our proposed CEKD scheme with the previously proposed key distribution schemes in terms of computational cost. The computational cost is defined as the total time required for the vehicle user to get the group key from the TA. The computational cost of CEKD scheme is compared with many existing schemes, namely DIKE (Lu *et al*., 2012), ID-AGKA (Du *et al*., 2003), HPF-CLGKA (Xiaozhuo *et al*., 2015) and Teng's scheme [Teng and C.K Wu]. Let us consider T_p represents the time required for performing a pairing operation, T_h represents the time required for performing a hash operation and T_m represents the time required for performing point multiplication.

For performing the hash operation, point multiplication and pairing operation, the pairing-based cryptography (PBC) library [Pairing-Based Cryptography] is used in this paper. For the aforementioned operations, the Type-A curve defined in the PBC library is used with the default parameters. In order to measure the actual computation time of our proposed CEKD scheme, we have used a 2-GHz machine with 4-GB installed memory, running Cygwin 1.7.35–15 [Cygwin] with the gcc version 4.9.2 for our implementations.

All the results are analyzed over 100 randomized simulation runs and then the average of the results is considered. In our simulations, the time parameters T_p, T_h and T_m are measured and it is found to be equal to 1.6 ms (milliseconds), 2.7 ms, and 0.001 ms, respectively.

Table II: Computational Cost of Various Key Distribution Schemes

Method	For one user	For n users
DIKE	$3T_p + 2T_h$	$(2n+1)T_p + 2nT_{h_h}$
ID-AGKA	$4T_p + 6T_m$	$4nT_p + n(n+1)T_m$
HPF-CLGKA	$9T_m + 2T_h$	$9nT_m + 2nT_h$

Teng's scheme	$2T_p + 2T_m + T_h$	$2nT_p + 2nT_m + nT_h$
CEKD (PROPOSED)	$2T_p + T_m$	$2nT_p + nT_m$

From Table II, it can be observed that our proposed CEKD scheme requires only two pairing and one point multiplication operation to get the gk from the TA and hence CEKD takes low computational cost compared to other existing schemes.

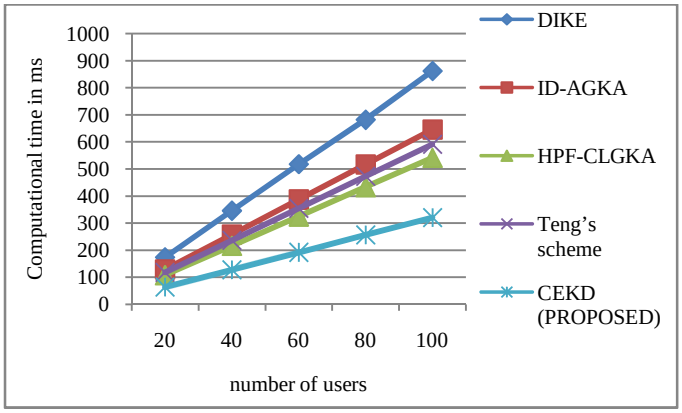

Fig. 2: Computational cost for key distribution

From Fig.2, it is very clear to understand that our proposed CEKD scheme takes only 320 ms for a secure group key distribution from the TA to the vehicle user. However, other existing schemes take more than 500 ms for secure group key distribution.

Conclusion:

In this paper, we have proposed CEKD scheme for secure group key distribution in VANETs. In order to avoid the man-in-the-middle attack, the TA performs the authentication process for each vehicle user V_i before distributing the group key. The security analysis section shows that the weaknesses of previously proposed schemes can be overcome by the proposed CEKD scheme and hence satisfies the security requirements. The performance analysis section shows that the proposed CEKD scheme takes low computational cost which makes it suitable for the VANET environment.

REFERENCES

Zhang, C., R. Lu, X. Lin, P.-H. Ho and X. Shen, 2008. An efficient identity- based batch verification scheme for vehicular sensor networks. in Proc. IEEE INFOCOM, Phoenix, AZ, USA: 246-250.

DSRC, http://grouper.ieee.org/groups/scc32/top_lvl3.html

Sun, Y., R. Lu, X. Lin, X. Shen and J. Su, 2010. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Trans. Veh. Technol., 59(7): 3589-3603.

Joux, 2000. A one round protocol for tripartite Diffie-Hellman. 2000. Proc. ANTS IV, LNCS 1838, Springer-Verlag pp: 385-394.

Lu, R., X. Lin, X. Liang and X. Shen, 2012. A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANET. 13(1): 127-139.

Du, X., Y. Wang, J. Ge and Y. 2003. Wang ID-based Authenticated Two Round Multi-Party Key Agreement. Cryptology ePrint Archive: Report.

Xiaozhuo, G., C. Zhenhuan and W. Yongming. 2015. How to Get Group Key Efficiently in Mobile Ad Hoc Networks?. Military Communications Conference, MILCOM, IEEE: 1009-1014.

Teng J.K., and C.K. Wu, 2012. A Provable Authenticated Certificateless Group Key Agreement With Constant Rounds. Journal of Communications and Networks, 14(1): 104-110.

Pairing-Based Cryptography [PBC] Library. [Online]. Available: http://crypto.stanford.edu/pbc/

Cygwin: Linux Environment Emulator for Windows. [Online]. Available: http://www.cygwin.com/

Hao, Y., Y. Cheng and K. Ren, 2008. Distributed key management with protection against RSU compromise in group signature based VANET. IEEE GLOBECOM.