IOP Conference Series: Earth and Environmental Science

PAPER • OPEN ACCESS

A Lightweight Secure and Efficient Authentication and Key Agreement Protocol for VANET

A Lightweight Secure and Efficient Authentication and Key Agreement Protocol for VANET

Yuxia Zhang and Fengtong Wen*

School of Mathematical Sciences, University of Jinan, Jinan Shandong, China
zhangyuxia90626@163.com, wftwq@163.com

Abstract. The vehicular ad hoc network (VANET), as an important part of the intelligent transportation system, has a crucial impact on traffic safety and efficiency. And its security issues have attracted many researchers. The secure communication among entities is particularly important due to the openness of the VANET environment. In this paper, we propose a lightweight secure and efficient authentication and key agreement protocol for VANET in order to implement secure communication. The scheme only uses lightweight computation to achieve anonymity, integrity and mutual authentication among entities.

1. Introduction

With the number of road vehicles has increased rapidly, and the role of vehicles in people's daily lives has become more and more important. Security issues are becoming more and more serious, while bringing convenience to people's lives. In order to reduce traffic accidents, researchers have proposed the concept of VANET [1]. It realizes the interactive communication between Vehicle to Vehicle (V2V) and Vehicle to infrastructure (V2I) through wireless communication improves driving. So far, VANET has no fixed architecture [2]. However, most vehicle authentication protocols in VANET are based on the common strategy of the Dedicated Short Range Communications (DSRC) protocol [3–4]. It provides the potential to effectively support VANET secure communications.

In recent years, many authentication and key agreement schemes have been proposed [5–10]. In 2005, Raya et al. [11] proposed an anonymous authentication scheme for VANET by using an anonymous certificate. But, vehicles need to have large storage space to store keys and certificates. In 2008, Zhang et al. [12] proposed an identity-based identity authentication scheme by using identity-based public key cryptosystem. However, their solutions do not provide non-repudiation capabilities and are vulnerable to relay attacks and impersonation attacks. In 2011, Chim et al. [13] proposed an identity-based authentication scheme with two shared secrets. Their approach provides anonymity to users and has lower communication costs.

The rest of the paper was organized as fallow. We describe the system model and security requirements in Section 2. In Section 3, we describe our new proposed authentication scheme. Section 4, We describe the performance analysis of this scheme. Finally, we give the conclusion of the paper in section 5.

2. System Model and Security Requirements

2.1. System Model

In our scheme, the system model consists of four parts: trust authority (TA), road side unit(RSU), on board unit(OBU) and tamper-proof device(TPD).

TA: TA is completely trusted by other entities. TA is charge of the registration of all entities and responsible for generating the session key and verifies the identity. It is responsible for publishing system parameters and data writes.

RSU: The RSU is a semi-trusted entity. It assists TA in completing various tasks. Each RSU is embedded with a TPD that records the necessary information.

OBU: The OBU is embedded in the vehicle and is responsible for collecting collecting traffic information.

TPD: The TPD is used to store cryptographic material and handle cryptographic operations. In any case, all data stored in it cannot be extracted by the adversary. It only allows the TA to write information when our program is registered.

2.2. Security Requirements

(1) Message authentication and integrity: In VANET, the sender sends out every message that should be authenticated by the recipient to ensure that the message has not been modified or forged by an unauthorized adversary.

(2) Conditional privacy preserving: In VANET, the real identity of each vehicle should not be exposed to any other entity. TA should have the authority to get the real identity of the initiator through valid information.

(3) Resist malicious attacks: To ensure security, an authentication scheme is resistant to a variety of malicious attacks, such as forgery attack, replay attacks and so on.

3. Our Proposed Scheme

In this section, we propose a lightweight secure and efficient authentication and key agreement protocol for VANET. Our scheme consists of four phases: initial phase, registration phase, login and authentication phase and password-change phase. In this protocol, addition of new node also needs to register. The details are as follows:

3.1. Initial Phase

In this phase, TA chooses a $s \in Z_q^*$ as its own private key. Then, it selects a hash function $h(\cdot)$, an encryption function $E_x(\cdot)$ and publishes them.

3.2. Registration Phase

Vehicle registration phase *Step 1.* For each vehicle node V_i selects a unique identity ID_i and a secure password PW_i. It chooses a nonce number $n_i \in Z_q^*$ and send $\{ID_i, n_i\}$ to the TA via a secure channel.

Step 2. Upon receiving the message $\{ID_i, n_i\}$ from V_i, the TA uses its own private key to calculate $A_i = h(ID_i \| s)$ and $B_i = h(n_i \| s)$. Then, $E_s(n_i)$ is handled by encrypting n_i with the private key s of TA. After that, TA embedded the information $\{A_i, E_s(n_i),$ $B_i\}$ into an OBU_i and sends the OBU_i to V_i via a secure channel.

Step3. Upon receiving the OBU_i from TA, OBU_i computes $VP_i = h(ID_i \| A_i)$, $VQ_i = h(PW_i \| A_i)$, $C_i = h(VP_i \| VQ_i)$ and $F_i = B_i \oplus C_i$ and stores the message $\{A_i, C_{i,}, F_i, E_s(n_i)\}$ instead of the previous message. After that, the owner of V_i is attaching OBU_i to the V_i.

RSU registration phase *Step 1.* The node RSU_j chooses his identity RID_j and a random number $r_j \in Z_q^*$. Then it sends $\{RID_j, r_j\}$ to TA through a secure channel.

Step2. When TA receives the message $\{RID_j, r_j\}$ from RSU_j, the TA uses its own private key s to calculate $RA_j = h(r_j \| s)$ and $RB_j = RA_j \oplus h(RID_j \| r_j)$. After that, TA stores the message $\{RB_j, r_j\}$ in TPD and delivers it to RSU_j.

Step3. Upon receiving the TPD, RSU_j stores it.

3.3. Login and Authentication Phase

In this phase, we describe the login and authentication process as follows.

Step1. The owner of V_i enters ID_i and PW_i into the OBU_i. Then, OBU_i computes $VP_i^{'} = h(ID_i \| A_i)$, $VQ_i^{'} = h(PW_i \| A_i)$ and $C_i^{'} = h(VP_i^{'} \| VQ_i^{'})$, and verifies whether $C_i^{'}$ is the same as C_i stored in it. If $C_i^{'} \neq C_i$, then the OBU_i will ask the owner of V_i to enter the correct identity and password again. Otherwise, OBU_i computes $B_i = F_i \oplus C_i^{'}$. After that, OBU_i chooses a current timestamp T_1, computes $Y_1 = h(B_i \| T_1) \oplus ID_i$, $Y_2 = h(Y_1 \| B_i \| ID_i \| T_1)$ and sends $\{T_1, Y_1, Y_2, E_s(n_i)\}$ to the RSU_j through a public channel.

Step2. Upon receiving the message, RSU_j checks the freshness of T_1. If it is invalid, RSU_j terminates this phase and sends a rejection message to $OBU_i^{'}$ .Otherwise, it computes $RA_j = RB_j \oplus h(RID_j \| r_j)$, in which RB_j is stored in RSU_j's TPD. Again, it chooses a current timestamp T_2 and computes $AID_j = RID_j \oplus h(RA_j \| T_2)$, $Y_3 = h(RB_j \| T_2)$, $Y_4 = h(RID_j \| Y_3 \| T_2)$ and then sends $\{T_1, Y_1, Y_2, E_s(n_i), T_2, Y_3, Y_4, r_j, AID_j\}$ to the TA through a public channel.

Step3. When TA receives message, it first verify the validity of T_2. If it is valid, TA computes $RA_j^{'} = h(r_j \| s)$, $RID_j^{'} = AID_j \oplus h(RA_j^{'} \| T_2)$, $RB_j^{'} = RA_j^{'} \oplus h(RID_j \| r_j)$ and $Y_3^{'} = h(RB_j^{'} \| T_2)$. After that, it calculates $Y_4^{'} = h(RID_j^{'} \| Y_3^{'} \| T_2)$ whether is equal to the Y_4 received. If it is equal, RSU_j is authenticated. TA also uses master key s to decrypt $E_s(n_i)$, then computes $B_i^{'} = h(n_i \| s)$, $ID_i^{'} = Y_1 \oplus h(B_i^{'} \| T_1)$, $A_i^{'} = h(ID_i^{'} \| s)$ and $Y_2^{'} = h(Y_1 \| B_i^{'} \| ID_i^{'} \| T_1)$. If $Y_2 = Y_2^{'}$, only then the TA can verify the identity of OBU_i. Otherwise, it terminates the session. So far, OBU_i and RSU_j have been certified by TA. Then, it chooses a current timestamp T_3 and a session key(SK), then it masks SK for OBU_i by computing $Y_5 = SK \oplus h(A_i^{'} \| B_i^{'} \| T_3)$, as well as masks SK for RSU_j by computing $Y_6 = SK \oplus h(RA_j^{'} \| T_3)$. Finally, it continues to compute $Y_7 = h(Y_5 \| A_i^{'} \| T_3)$, $Y_8 = h(Y_6 \| T_3 \| RA_j^{'})$ and sends $\{T_3, Y_5, Y_6, Y_7, Y_8\}$ to RSU_j via a public channel.

Step4. When receiving the response message, RSU_j first verifies whether the timestamp T_3 is valid. RSU_j Computes $SK^{'} = Y_6 \oplus h(RA_j^{'} \| T_3)$ and $Y_8^{'} = h(Y_6 \| T_3 \| RA_j)$. RSU_j checks whether $Y_8^{'}$ equals to Y_8 or not. If it is valid, TA is authentic. After that, it computes $Y_9 = h(SK^{'} \| Y_5 \| T_4)$ where T_4 is RSU_j's current time. Finally, RSU_j sends $\{T_3, T_4, Y_5, Y_7, Y_9\}$ to OBU_i.

Step5. Upon receiving message, OBU_i verifies the validity T_4. If it is permitted, RSU_j calculates $Y_7^{'} = h(Y_5 \| A_i \| T_3)$ and verify that Y_7 and $Y_7^{'}$ are equal. If it is hold, TA is authentic and OBU_i gets $SK^{'} = Y_5 \oplus h(A_i \| B_i \| T_3)$. Subsequently, OBU_i checks whether $Y_9^{'} = h(SK^{'} \| Y_5 \| Y_7^{'} \| T_4)$ equals to the received Y_9 to decide whether accept the session key. If it is equal, OBU_i will believe that there is a session key between OBU_i and RSU_j. In summary, the login and authentication phases are completed.

3.4. Password Change Phase

Step1. V_i enters his identity ID_i and password PW_i into a terminal device of OBU_i. Then, OBU_i calculates $B_i^{'} = F_i \oplus C_i^{'}$ $VP_i = h(ID_i \| A_i)$, $VQ_i = h(PW_i \| A_i)$ and $C_i^{'} = h(VP_i \| VQ_i)$ and checks if the calculated $C_i^{'}$ is equal to the value C_i stored in.

Step2. If they are not equal, this request is rejected; otherwise, OBU_i asks V_i to enter the new password PW_i^{new}. After getting PW_i^{new}, OBU_i computes $VQ_i^{new} = h(PW_i^{new} \| A_i)$, $B_i^{'} = F_i \oplus C_i^{'}, C_i^{new} = h(VP_i \| VQ_i^{new})$ and $F_i^{new} = B_i^{'} \oplus C_i^{new}$.

Step3. OBU_i replace C_i and F_i with C_i^{new} and F_i^{new} separately in its memory.

4. Property Analysis

Mutual authentication. In our scheme, TA gets the vehicle $ID_i^{'}$ by computing $ID_i^{'} = Y_1 \oplus h(B_i^{'} \| T_1)$ and $B_i^{'} = h(n_i \| s)$, then gain $A_i^{'} = h(ID_i^{'} \| s)$, which is equal to the storage in the OBU_i's secret value A_i. Simultaneously, TA compares $Y_2^{'}$ to Y_2 to authenticate V_i. V_i can also authenticate TA by computing the Y_7, which has the secret $A_i^{'}$ only known by TA and V_i. The mutual authentication between RSU_j and TA is similar to the authentication between V_i and TA.

Anonymity. The vehicle's ID_i is hidden in A_i and Y_1. There are two unknown values in A_i that are difficult to guess at the same time for an attacker. So, it is difficult to get $ID_i \cdot Y_1 = h(B_i \| T_1) \oplus ID_i = h(h(n_i \| s) \| T_1) \oplus ID_i$ where the s is only known by TA. So, it's also hard to obtain ID_i.

Replay attack. The replay attack is caused when a malicious vehicle intercepts the message of the previous session and replays it in the current session to imitate the legitimate vehicle. In our proposed scheme, the information we transmit on the channel already contains the timestamp of the protection replay attack. The timestamp T_i is used to maintain the freshness of the message transmitted on the channel. Entities in the system can then verify these timestamps to detect replay attacks. In summary, our proposed scheme provides resistance to replay attacks.

Traceability. From the previous analysis, we can find that only the TA can be done to reveal the true identity of the vehicle node V_i and the node RSU_j. Therefore, when a malicious event occurs TA can track them based on malicious information.

5. Conclusion

In this paper, we present a lightweight secure and efficient authentication and key agreement scheme for VANET. In this scenario, our generated session key has its own unique advantages. And, we do not use complex operations and calculations, only simple calculations such as XOR operations or hash functions that make calculations more efficient and feasible. Therefore, it reduces costs and delays. We also enable authentication of RSU and high-speed mobile vehicles. In addition, the vehicle node and RSU do not need to occupy storage space to store the shared key and identity at the TA.

6. Acknowledgements

This study was supported by the National Science Foundation of Shandong Province (No. ZR2018LF006).

7. References

[1] Li F., Wang Y.. Routing in Vehicular Ad Hoc Networks: A Survey. IEEE Vehicular Technology Magazine. vol. 2, pp. 12--22 (2007)
[2] Toor Y., Muhlethaler P., Laouiti A.: Vehicle ad hoc networks: Applications and related technical issues, IEEE Commun. Surv. Tutor. vol. 10, pp. 74--87 (2008)
[3] Bayat M., M. Barmshoory, M. Rahim, Aref M.R.: A secure authentication scheme for vehicular ad hoc networks with batch verification, Wirel. Netw. vol. 21, pp. 1733--1743 (2014)
[4] Shim K.A.: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks, IEEE Trans. Veh. Technol. Vol. 61, pp. 1874--1883 (2012)
[5] Wang C.,Xu G.: Crypt analysis of three password-based remote user authentication schemes with non-tamper-resistant smart card. Security and Communication Networks, vol. 2017, DOI:https://doi.org/10.1155/2017/1619741
[6] Huang X, Chen X, Li J, et al.: Further Observations on Smart-Card-Based Password Authenticated

Key Agreement in Distributed Systems. J. IEEE Transactions on Parallel and Distributed Systems 2014, vol. 25. pp. 1767--1775 (2014)
[7] Ma C, Wang D, Zhao S.: Security flaws in two improved remote user authentication schemes using smart cards. J. International Journal of Communication Systems 2015, vol. 27. pp.2215--2227 (2015)
[8] D. Wang, D. He, P. Wang, and C. Chu.: Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment, IEEE Transactions on Dependable and Secure Computing, vol. 12, pp. 428--442 (2015)
[9] Wang D, Wang P.: On the anonymity of two-factor authentication schemes for wireless sensor networks.J. Computer Networks 2014, vol. 73, pp. 41--57 (2014)
[10] Wen F., Susilo W., Yang G.: A Robust Smart Card Based Anonymous User Authentication Protocol for Wireless Communications. Security Communication Networks. Vol. 7, pp. 987--993. (2014)
[11] Raya M., Hubaux J.P.: Securing vehicular ad hoc networks, Journal of Computer Security, vol. 15, pp. 39--68 (2007)
[12] Zhang C., Lu R., Lin X. et al.: An efficient identity-based batch verification scheme for vehicular sensor networks, AZ, pp.816--824. Proc. of IEEE INFOCOM08, Phoenix, (2008)
[13] Chim T., Yiu S., Hui L., Li V.: SPECS: Secure and privacy enhancing communications schemes for VANETs, Ad Hoc Netw. vol. 9, 189--203 (2011)