An Efficient Privacy Preservation in Vehicular Communications Using EC-Based Chameleon Hashing

Christo Ananth, Assistant Professor, Department of Electronics & Communication Engineering, Francis Xavier Engineering College, Tirunelveli, India.

Dr. S. Selvakani, Assistant Professor, Department of Computer Science/Computer Applications, Tiruvalluvar University Constituent College of Arts and Science, Attupakkam, Arakkonam, India.

K. Vasumathi, Assistant Professor, Department of Computer Science/Computer Applications, Tiruvalluvar University Constituent College of Arts and Science, Attupakkam, Arakkonam, India.

Abstract--- The activity related status data will be communicated consistently and shared among drivers through VANETs keeping in mind the end goal to enhance driving security and solace. Along these lines, Vehicular specially appointed systems (VANETs) require safeguarding and secure information correspondences. Without the security and protection ensures, the aggressors could track their intrigued vehicles by gathering and breaking down their movement messages. A mysterious message confirmation is a basic prerequisite of VANETs. To conquer this issue, a protection safeguarding confirmation convention with expert traceability utilizing elliptic bend based chameleon hashing is proposed. Contrasted and existing plans Privacy saving confirmation utilizing Hash Message verification code, this approach has the accompanying better elements: common and unknown validation for vehicle-to-vehicle and vehicle-to-roadside interchanges, vehicle unlinkability, specialist following capacity and high computational effectiveness.

I. Introduction

To make a versatile system, the vehicular impromptu system (VANET) utilizes autos as portable hubs in a MANET. It makes a system with a wide range by considering each taking part vehicle into a hub or remote switch, permitting the vehicles around 100 to 300 meters of each other to interface and spreads an extensive variety of correspondence [1]. It is assessed that the main frameworks that will incorporate this innovation are police and fire vehicles to speak with each other for security purposes. To give security and different applications to the drivers and also travelers, VANETs are the promising methodology. It turns into a key segment of the smart transport framework [3]. A considerable measure of works have been done towards it however security in VANET got less consideration. Security got less consideration among every one of the difficulties in the VANET. In Vehicular Adhoc Network the parcels contains life basic data. In this way, it is important to ensure that these bundles are not embedded or altered by the programmer or aggressor; and furthermore the risk of drivers ought to likewise be built up at activity condition effectively and inside time. These sorts of security issues are don't like general correspondence arrange. It relies on upon the measure of system, geographic significance, versatility and so forth makes the usage troublesome and unmistakable from other system security.

The vast majority of the calculations are acquainted in writing with give security in VANET to both correspondences like vehicle to vehicle and vehicle to framework. For giving security the elliptic bend cryptography (ECC) standard and [2] RSU-helped message verification plot named RAISE [3] is presented by zhang, lin et all. It creates activity overhead and delivers little deferral and movement. In RAISE, vehicles can't advise their genuine personalities to each other, though RSUs can recognize whether two messages are sent by a similar vehicle. The TA and RSUs participate, which can follow the genuine personality of a message sender. Each vehicle needs to check the declaration repudiation list (CRL) to abstain from speaking with disavowed vehicles and after that confirm the sender's gathering mark to check the legitimacy of the got message while getting a message from an obscure element,. The current frameworks utilizes hash message confirmation coding (HMAC) [4] to supplant the CRL, consequently enormously decreasing the checking time to address the CRL checking issue. Be that as it may, both of these depend on pen names, may not fit gathering mark based plans specifically. Xiaoyan Zhu, Shunrong Jiang et all presents a productive restrictive security safeguarding validation plot for VANETs [1] under the semi-trust model of RSU is exhibited by mutually utilizing the strategies the accompanying procedures. The systems give HMAC, clump gather signature check and additionally helpful validation. This plan first partitions the region into a few areas so that the framework can keep running in a limited way. It figures HMAC with advanced mark calculation where
the gathering key produced by the self-recuperating bunch key era calculations, which can supplant the tedious CRL checking and guarantee the respectability of messages before cluster confirmation. In any case, this plan does not give unknown validation in VANETs, V2V and V2R shared verification, vehicle unlinkability, productivity.

In this paper a protection saving confirmation convention with specialist traceability utilizing elliptic bend based chameleon hashing is proposed. It improves the security and protection of vehicles by giving both V2R and V2V common confirmation. It understands the time-differing unknown endorsements, by update the chameleon signature and incorporates it with EC computerized signature calculation. The Elliptic Curve-based chameleon hash signature, whose one of a kind elements not just guarantee the protection and security of VANET interchanges additionally enhance the execution of VANET correspondence because of its low intricacy in character check.

II. System Model

As appeared in Fig. 1, the framework demonstrate under thought comprises of the accompanying: A Certificate Authority, which is in charge of giving mysterious declarations and circulating mystery keys to all OBUs in the system. Settled RSUs are at the street side, and the OBUs prepared on running vehicles. The enrollment and accreditation place for RSUs and OBUs are Certificate Authority. The CA just can recoup the genuine personality of an OBU from its endorsement. The go-between amongst OBU and CA is RSUs that work in a semi-trusted manner since they are conveyed at unattended roadsides. RSU is in charge of separating fake messages from noxious or renounced vehicles and revealing OBU's authentication data to CA. The movement related status data (e.g., speed, area and increasing speed) is communicated intermittently to help drivers with a superior consciousness of their driving condition.

![Fig. 1: System Model](image)

III. EC-Based Chameleon Hash Signature

The proposed validation calculation depends on Chameleon signature. Be that as it may, the attributes of these mark calculations are non-intelligent. That implies the mark can be produced without connecting with the proposed beneficiary. Along these lines, the execution of verification can be fundamentally made strides. Be that as it may, the ordinary discrete logarithm based computerized chameleon hash signature calculations [8] require a similar open key issued by the underwriter for check. The programmers may hack this open key, accordingly it doesn't ensure the unlinkability. With a specific end goal to address this issue, the chameleon hash mark is upgraded that abstains from utilizing the settled open keys.

The enhanced rendition is based upon an Abelian gather $G_p$ framed by the focuses on the elliptic bend as defined, where $p$ is an expansive prime number. For security thought, the cardinality of $G_p$, i.e., $|G_p|$, ought to be distinguishable by a vast prime number $q$. A point $P$ browsed $G_p$ alongside the numbers $p$ and $q$ are distributed by the trust specialist as framework parameters meant as $(p, P, q)$. In the accompanying, we display the validation procedure between a prover and a verifier utilizing EC-based chameleon hash signature.

Initially, the prover generates its chameleon $C \in G_p$ as $C = S \cdot P$, where $S$ is randomly chosen from $[1, q - 1]$ as secret information to the prover. Once the prover needs to be authenticated by the verifier, it generates a new private key $\alpha$ randomly chosen from $[1, q - 1]$ and then obtains the corresponding public key $y$ as $y = \alpha$. After that, an auxiliary parameter $m$ is found by the collision finding algorithm $CFind(\alpha, nonce, S)$ algorithms as
m = CFind(α, nonce, S) = S - αy (1)

γ = h(y ⊕ nonce) (2)

where nonce is the recent challenge provided by the prover and h(.) is a strong one-way hash function, mapping strings of arbitrary length to a number in [1, q - 1]. Finally, the prover sends (C, m, y, nonce) to the verifier for authentication. At the verifier side, the received information (C, m, y, nonce) is used to authenticate the prover by checking if CH(m, y, nonce) is equal to C, where the chameleon hash function CH(m, y, nonce) can be computed as

CH(m, y, nonce) = m . P + γ.

= m . P + h(y ⊕ nonce) . y (3)

If CH(m, y, nonce) = C holds, the verifier passes the authentication for the prover. Otherwise, the prover will be considered as hacker. For a valid user, the authentication is always successful. It can be confirmed by substituting (1) to (3)

CH(m, y, nonce) = m . P + γ.

= (S - αy) . P + γα . P = S . P = C (4)

In the proposed signature scheme, the public key y is updated at each authentication session. This scheme shall show in a later section how this EC-based chameleon hash signature can meet all security requirements of VANETs.

A. Registration Phase

Both OBUs and RSUs need to be registered with CA. In this registration phase of OBU b, it generates random number S b ∈ [1, q - 1] as its secret key and sends its initial chameleon C b = S b . P and its real identity ID b to CA. On receiving the registration request, CA produces a certificate CER b for OBU b as

CER b = Sign(C b, KCA) (5)

Using its private key KCA by signing Cb. The information (CER b, IDb) is then stored in the database of CA and CER b will be sent back to OBU b through a secure channel. The certificate of RSU a is generated as

CER a = Sign(C a, KCA) (6)

where C a = S a . P.

B. V2R Mutual Authentication Phase

In this phase, RSU a initiates the authentication with OBU b and then they both establish a pair-wise key between each other. The mutual authentication phase is elaborated as follows. Without loss of generality, we consider a mutual authentication at session i. RSU a generates a new private key a i with the corresponding public key y a i = a i . P that is different from the previous one so as to avoid the linkability problem. Then the auxiliary parameter m a i is updated by m a i = C. Find(a i, T a i, S a) where T a i is the current time. Finally, the information (CER a, m a i, y a i, T a i) i is sent to OBU b for verification. Upon receiving this information, OBU b uses the public key KCA of CA to verify the legitimacy of RSU a by checking:

Verify(CER a, KCA) = CH(m a i, y a i, T a i) (7)

If RSU a passes the verification, i.e., the above equation holds, a pair-wise K a b i is generated as

K a b i = a i . y a i (8)

To achieve mutual authentication, OBU b should be also verified by RSU a following a similar process. The only concern is that the certificate CER b of OBU b cannot be sent to RSU a directly, because each certification is unique and can be used for tracking by adversaries. For this reason, certificate CER b along with the current time T b is encrypted by K a b as

CER b = Encrypt(CER b ⊕ T b, K a b) (9)

That guarantees unlinkability of OBU b. Finally, the information (CER b, m b i, y b i, T b) is sent to RSU a to complete the mutual authentication. Using the received information, RSU a also obtains the same pair-wise key K a b i = a i . y a i because

K a b i = a i . y a i = a i . (a i . P) = a i . (a i . P)
Therefore, certification $CER_b$ can be recovered by decrypting $CER_b$ using pair-wise key $K_{2b}^{(i)}$ i.e.,

$$CER_b = \text{Decrpt}(CER_b, K_{2b}^{(i)})$$

(11)

Note that the freshness of $T_{2b}^{(i)}$ should be examined. Moreover, RSU$_a$ needs to check if $CER_b$ is in the revocation list that is retrieved from CA. If in the list, RSU$_a$ terminates the mutual authentication session immediately. Otherwise, the legitimacy of OBU$_b$ can be verified by checking if

$$\text{Verify}(CER_b, K_{2b}^{(i)}) = \text{CH}(m_b^{(i)}, y_b^{(i)}, T_{2b}^{(i)})$$

(12)

holds. After that, the mutual authentication process completes.

C. V2V Mutual Authentication Phase

There is no protection issue required for RSUs in V2R verification stage, so their unique declarations are conveyed specifically for the validation reason. The principle contrast in V2V validation stage is that the endorsement of each gathering must be scrambled with some fluctuation to such an extent that the subsequent declaration adjusts each time and the first testament can be recouped by a lawful beneficiary at confirmation session. To accomplish this objective, the V2V shared confirmation stage comprises of 1) private key trade for pairwise key era and 2) encoded accreditation trade and check. This plan considers a shared confirmation amongst OBU$_a$ and OBU$_b$ at session $i$. Toward the start of the session, a refreshed private key is created at each side and the relating open key incorporated into their periodical signal messages. After the key exchange, each party calculates their pair-wise key independently such that

$$K_{2b}^{(i)} = a_b^{(i)}, y_b^{(i)} = a_b^{(i)}, y_b^{(i)} = K_{2b}^{(i)}$$

At eachide, e.g., OBU$_a$, the information $(K_{2b}^{(i)}, y_b^{(i)})$ for session $i$ is maintained in a pairwise key table at OBU$_a$. Then the pairwise key is used to produce encrypted certificates $CER_b = \text{Encrpt}(CER_b \oplus T_{2b}^{(i)}, K_{2b}^{(i)})$ and $CER_b = \text{Encrpt}(CER_b \oplus T_{2b}^{(i)}, K_{2b}^{(i)})$ at OBU$_a$ and OBU$_b$, respectively. Another round of message exchange is required by passing the encrypted certificate as well as other information for verification to each other. For example, after receiving $(CER_b, y_b^{(i)}, m_b^{(i)}, T_{2b}^{(i)})$, OBU$_a$ first looks up its pairwise key table for the entry relating to $y_b^{(i)}$ and the corresponding pairwise key $K_{2b}^{(i)}$ is then used to recover the original certificate $CER_b$. The remaining verification process for each OBU is then conducted in a similar manner as described in the V2R case.

D. CA Tracking Phase

The CA Tracking phase is launched only when dealing with a dispute event. Once the real ID of an OBU needs to be recovered, its CER will be reported to CA. Since each CER is unique, CA can lookup its database to find the identity of corresponding to OBU.

IV. Performance Analysis

This section provides the performance analysis of secure vehicular authentication scheme. Fig 2 shows the network formation of the WSN. Here the simulations are done in Ns2 simulator. First the hello packets are transmitted between all nodes. The keys for vehicles as well as road side unit are distributed during hello packet transmission. Thus the registration of the RSU and the Vehicles real identity is done to the central authority and certificates are issued.

![Registration Phase](image)
Fig 3 shows that the V2V communication in network. Here the vehicles can broadcast the emergency message securely to its neighbors within a correct time. The proposed chameleon hash signatures can securely transmit the messages between vehicles.

Fig. 3: V2V Communication

Fig 4 shows that the V2I communication in network. The vehicles can broadcast the messages to road side unit named as infrastructure when the destination vehicle is apart from its range. The road side unit can broadcast the messages to that corresponding vehicle. The proposed chameleon hash signature can achieve both V2V and V2I communications.

Fig. 4: V2I Communication

Fig. 5: Delay
Fig. 5 and 6 shows that the delay and packet loss graph. The graph is plotted between time versus delay and time versus packet loss. Compared with existing scheme the delay and packet loss rate is reduced in the proposed scheme.

V. Conclusion

Vehicular impromptu systems (VANETs) require saving and secure information interchanges. Without the security and protection ensures, the assailants could track their intrigued vehicles by gathering and breaking down their movement messages. To give a mysterious message verification, a security safeguarding validation convention with specialist traceability utilizing elliptic bend based chameleon hashing is proposed. It can fulfill many wanted properties for secure and protection safeguarding vehicular interchanges. These plans additionally exhibit high proficiency of the proposed convention in various delegate vehicular correspondence situations by broad ns2-based reenactment. Contrasted with existing plans, the proposed convention can accomplish common verification for both V2R and V2V traffics with much lower computational cost, and henceforth is exceptionally reasonable in a practical vehicular condition. In future, this work can be stretched out by considering more test in V2V correspondence and V2I correspondence likewise direct more execution assessment on message end-to-end postpone and message misfortune proportion in V2V correspondence and V2I correspondence.

References

[1] Zhu, X., Jiang, S., Wang, L. and Li, H. Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks. IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY 63 (2) (2014).
[2] Mershad, K. and Artail, H. A framework for secure and efficient data acquisition in vehicular ad hoc networks. IEEE Trans. Veh. Technol. 62 (2) (2013) 536–551.
[3] Zhang, C., Lin, X., Lu, R., Ho, P.H. and Shen, X. An efficient message authentication scheme for vehicular communications. IEEE Trans. Veh. Technol. 57 (6) (2008) 3357–3368.
[4] Guo, J., Baugh, J.P. and Wang, S. A group signature based secure and privacy-preserving vehicular communication framework. Proc. Mobile Netw. Veh. Environ., 2007, 103–108.
[5] Sun, Y., Lu, R., Lin, X., Shen, X. and Su, J. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Trans. Veh. Technol. 59 (7) (2010) 3589–3603.
[6] Choi, J. and Jung, S. A handover authentication using credentials based on chameleon hashing. IEEE Communications Letters 14 (1) (2010).
[7] Zhang, J., Chen, H. and Geng, Q. A Secure Chameleon Hash Function without Key Exposure from Pairings. Proceedings of International Symposium on Web Information Systems and Applications, 2009, 015-018.
[8] Chen, X., Zhang, F., Susilo, W., Tian, H., Li, J. and Kime, K. Identity-Based Chameleon Hashing and Signatures Without Key Exposure. Elsevier Science (2013).
[9] Ateniese, G. and de Medeiros, B. Identity-Based Chameleon Hash and Applications. Proc. Financial Cryptogr, 2004, 164-180.
[10] Boneh, D. and Franklin, M. Identity-Based Encryption From the Bilinear Pairing. Berlin, Germany: Springer-Verlag (2001) 213-229.