Defence Science Journal, Vol. 71, No. 2, March 2021, pp. 192-199, DOI : 10.14429/dsj.71.15534

A Novel Pseudonym Assignment and Encryption Scheme for Preserving the Privacy of Military Vehicles

Righa Tandon* and P.K. Gupta

Department of Computer Science and Engineering, Jaypee University of Information Technology, Solan - 173 234, India
**E-mail: righatandon@gmail.com,*

ABSTRACT

In this digital era, security has become one of the important topics of concern, and things become more critical for military vehicles where safety plays a vital role. In this paper, we have discussed a pseudonym-based approach that preserves the real identity of military vehicles. This paper also focuses on military vehicles' location privacy by deploying a novel pseudonym assignment and encryption schemes. The proposed security scheme is based on a hybrid approach of matrix array symmetric key and the intelligent water drop scheme. After implementing the proposed security scheme, each military vehicle will obtain its pseudonym for hiding their original identities. The proposed algorithm effectively manages pseudonym generation and change requests for the local region and inter-region environment. The proposed security scheme not only provides secure communication and preservation of location privacy of military vehicles but also ensures their security against various attacks. Finally, the time efficiency of proposed algorithms is obtained for both local and inter-region requests. Comparative analysis shows that the proposed scheme is more efficient than other existing techniques.

Keywords: Encryption; Intelligent water drop; Military vehicles; Privacy; Pseudonym; Security

NOMENCLATURE

V_i	i^{th} vehicle
RSU_n	n^{th} RSU
TID_i^k	Vehicle i has k^{th} pseudonyms. , $\{TID_i^k\}_{k=1}^{w} = \{TID_i\}$
pu_{k_i}	key for vehicle v_i
$Cert_i$	V_i certificate
LT_j	j^{th} local pseudonym fog
LA_j	The local authority of LT_j
CA	Central authority
t_s	Timestamp of event

1. INTRODUCTION

With the rising instances of terrorist attacks in the past, the role of information security has become more critical and challenging in the defence field. In defence services, communication between military vehicles is carried out by sending broadcast messages, containing highly confidential data; therefore, they demand high security. These broadcast messages include details about the vehicle's location, imposing a significant threat to military vehicles' location privacy. In this paper, we have focused on enhancing the security of various military vehicles, including the private vehicles of defence personnel, by incorporating pseudonyms.

The use of pseudonyms helps in preserving the anonymity of military vehicles by securing the vehicle's location and original information. This initial information of the vehicle is shared between the sender and the receiver vehicles. At the same time, confidential information of the vehicle gets safely exchanged among military vehicles using pseudonyms. Another advantage of using a pseudonym is that it reduces the communication overhead between the vehicles. Chaurasia[1], *et al.* have also discussed some cases of using pseudonyms during the exchange of information in vehicular communication.

In the proposed vehicular framework, fog nodes have a local authority that helps, generates, and manages pseudonyms; ensures low latency and cost; and improves military vehicles' location privacy. We have implemented one of the swarm intelligence–based techniques known as the intelligent water drop scheme, which provides better response time and performance and extends the Cloud computation capabilities to the edge of the network, as discussed by Kamkar[2], *et al.* and Shah-Hosseini[3].

Further, the research highlights of this work can be summarised as follows:

- This work presents a security framework for the location and movement of the military vehicle.
- Implements the intelligent water drop scheme and matrix array symmetric key (MASK) for encryption, and decryption of the messages.
- Discusses the algorithms for pseudonym generation, allocation, and change requests in both local and inter-regions.
- Computes the pseudonym generation and allocation costs for both local and inter-region requests of vehicles.

2. RELATED WORK

This section includes various studies related to vehicular communication, and their applications, privacy preservation,

Received : 24 February 2020, Revised : 21 January 2021
Accepted : 07 February 2021, Online published : 10 March 2021

and authentication schemes for vehicular ad-hoc networks. Along with that a detailed discussion on the various security schemes required during vehicular communication has been also provided.

2.1 Asymmetric Cryptography Schemes

Asymmetric cryptography scheme ensures privacy of the vehicles. In asymmetric cryptographic techniques, pseudonyms are used for vehicle-to-vehicle communication. Papadimitratos[4], *et al.* have presented the pseudonym issuance process in public key infrastructure (PKI), which is similar to the certificate issuance process. The central authority issues the certificates to vehicles, whereas the providers provided pseudonyms. Pseudonyms given to vehicles are valid for a limited time as stated by Echler[5], *et al*. Vehicles requiring new pseudonyms for a variety of reasons may cause scalability issues. By issuing pseudonyms the vehicles are authenticated. Vehicle-to-vehicle communication using pseudonyms takes place using public-key cryptography, which has public key certificates and key pairs. Signature and certificate are exchanged between sender and receiver to be sure of each other's identity. Petit[6], *et al.* and Kang[7], *et al.* have used a short signature scheme to encrypt the data and place it on to the Cloud. Different vehicles receive a key and a certificate from a central authority located in the Cloud in this scheme. Also, a privacy-preserved pseudonym scheme has been proposed for safe and secure communication among vehicles. Here, restricted encryption and authentication mechanisms are used for assured communication among vehicles. Xiong[8], *et al.* have constructed an identity-based signcryption along with an equality test scheme, which enhances the vehicles' efficiency and security as it authenticates the messages shared among vehicles in the network. Along with that, Kumar[9], *et al.* have proposed a framework that uses lattice-based cryptography for secure communication among vehicles, which is efficient as its communication and computational cost are quite low.

2.2 Symmetric Cryptography Schemes

This scheme uses a hashed message authentication code in which the signer hashes message and a secret key. Jiang[10], *et al.* have done verification of the message authentication code. Once you know the secret key only then an operation is performed on the message. Petit[6], *et al.* have discussed vehicle-to-vehicle communication and symmetric authentication schemes that require less authentication time and less security overhead. Considering this advantage, symmetric cryptographic methods are being used for authentication in a vehicular ad-hoc network. Groza[11], *et al.* have applied identity-based cryptography based on group signatures for preserving the vehicles' privacy. Safavat[12], *et al.* have proposed an ECC-based ACO ad-hoc routing protocol that uses ECC cryptographic keys to find a safe and efficient vehicle routing path.

2.3 Pseudonym-Based Batch Authentication Schemes

Jing[13], *et al.* have proposed pseudonym batch authentication schemes for VANET. Identity-based batch verification is designed, based on bilinear pairing. By using this scheme, the verification delay for batch message signatures gets reduced. These schemes do not consider storage and communication overheads. Also, value-added services are provided to the vehicles using the ABAKA (anonymous batch authentication and key agreement) scheme. This scheme helps in authenticating the requests of different vehicles and generating keys for other vehicles. Huang[14], *et al.* and Lo[15], *et al.* have proposed a pseudonym-based batch authentication scheme without using bilinear pairing. This scheme has supported message integrity, traceability, and authentication. Also, this scheme helped in better time consumption. Zhang[16], *et al.* have proposed an efficient and effective anonymous batch authentication scheme for the vehicular network. This scheme provides privacy protection and satisfies various security requirements. To ensure privacy, Wang[17], *et al.* have proposed a hybrid conditional privacy-preserving method based on a PKI certificate and identity-based signature.

3. METHODOLOGY

In this section, a vehicular framework has been proposed to send and store the information of military vehicle's securely on to the Cloud using a Fog environment. The proposed methodology results in faster computation, storage, and low-latency communication among vehicles. A matrix array symmetric key (MASK) with an intelligent water drop (iwd) scheme has been applied for encrypting the data of military vehicles. The section is further divided into the following subsections:

3.1 Proposed Framework

The proposed framework is shown in Fig. 1, consisting of three layers known as the User layer, the Fog layer, and the Cloud layer for providing security and processing of data at each level. The role of these layers and their association with the proposed techniques are described as follows:

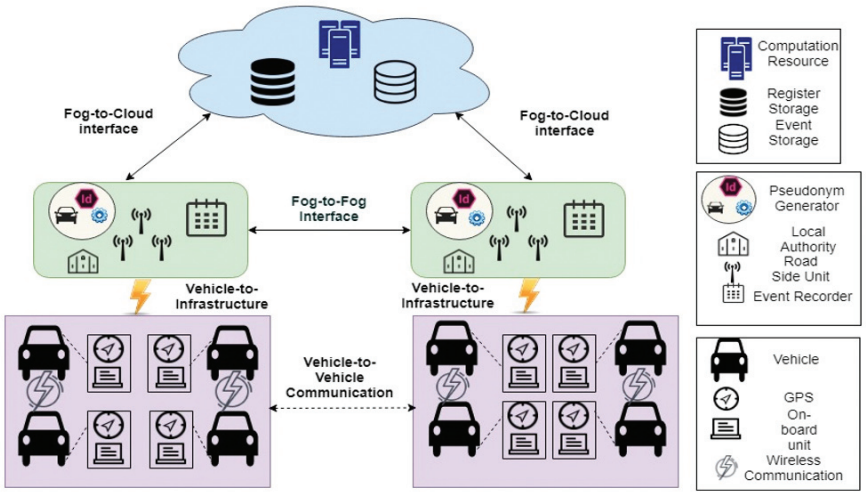

Figure 1. Proposed vehicle to vehicle communication framework.

- *Cloud layer*

This layer manages storage and computing resources and offers services to other layers through a central authority. The central authority first registers vehicles. The identity of any registered vehicle is encrypted using MASK and iwd schemes. All occurrences (events) are then stored in the event database.

- *Fog layer*

This layer provides all the services at the edge of the network. Here, each fog node has a pseudonym generator, roadside units (RSUs), a local authority, and an event recorder. The proposed pseudonym generator generates and stores pseudonyms for vehicles. The RSUs help in providing services to the edge of the network for the vehicles. The event recorder also aids in recording all the events that occurred including any misconduct of vehicles.

- *User layer*

In this layer, vehicles perform one to one communication and also with the fog infrastructure in wireless mode. Each vehicle is provided with onboard units and GPS. An onboard unit on any vehicle can communicate with a similar unit on another vehicle, while GPS helps in exchanging information between the vehicles and fog infrastructure.

3.2 Proposed Security Scheme

The proposed security scheme is presented in Fig. 2, which discusses the various steps for implementing the various security measures, including the registration process, encryption process, pseudonym assignment/change process, and decryption process. First, vehicle registration is done in the registration process. Here, for sending information of the vehicle to the Cloud, an encryption process is followed. Further, for assigning pseudonyms to different vehicles, the pseudonym process is carried out, and finally, in the decryption process, the real information of the vehicle, is accessed. The role of each process comprising the security model is described as follows:

- *Registration process*

First, vehicles requiring storage services from the Cloud register themselves with a real identity. Here, the vehicle's required information is obtained, and the registration process is completed by authenticating the vehicle.

- *Encryption process*

Information about the vehicle to be transferred to the Cloud is encrypted first. Here, for encryption purposes, both MASK and iwd schemes have been applied. This scheme implements the following steps for encrypting information:

- Matrix initialisation is used for generating keys by using MASK.
- Key scheduling is performed.
- Substitution and diffusion are done.
- Finally, the obtained key is used with the iwd scheme for encrypting the vehicle's information.

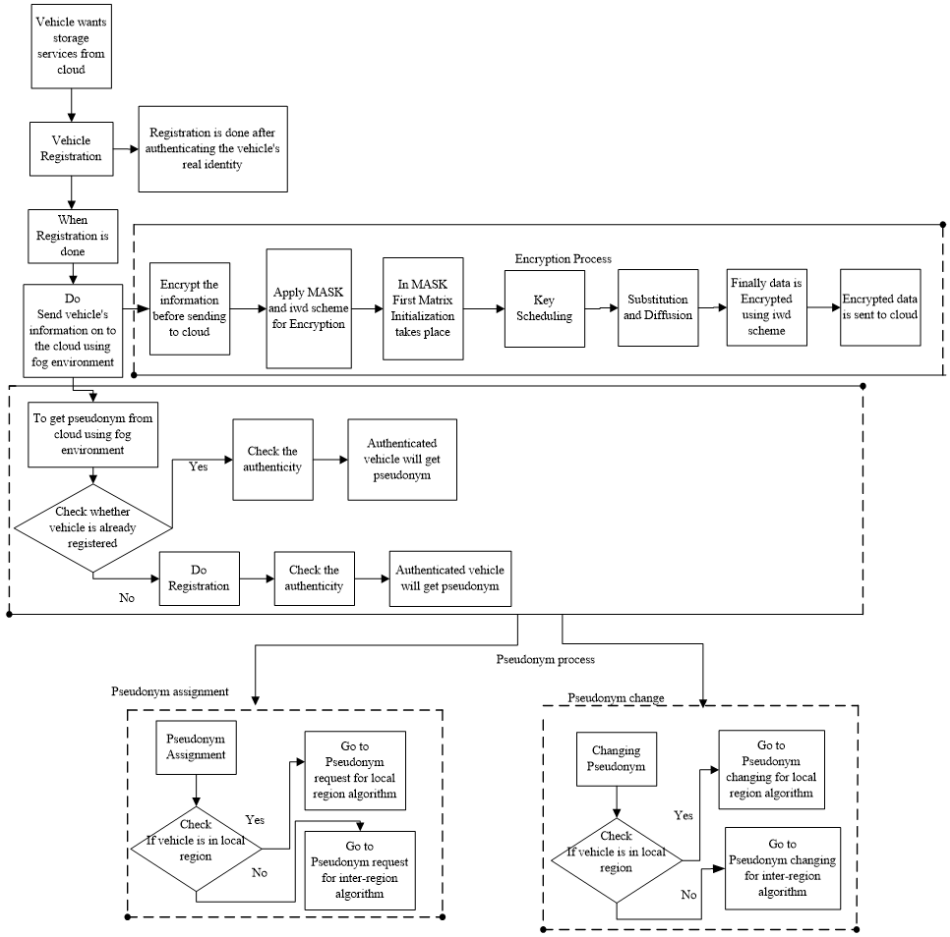

Figure 2. Proposed security scheme for secure communication in a vehicular network.

- *Pseudonym assignment/change process*

This process ensures more robustness and avoids revealing vehicles' real identities. The pseudonyms are assigned to vehicles using the fog environment, in which the vehicle's identity is checked with the database. Once the vehicle's identity is matched, its authenticity is checked, and a pseudonym is assigned to the requesting vehicle. However, if there is any failure, then vehicle registration is done, checked for authenticity, and finally, the pseudonym is assigned. This process consists of two sub-steps, i.e. pseudonym assignment and change:

Pseudonym Assignment: For assigning a pseudonym to the vehicle, the requested vehicle's location is checked first. If the vehicle is in the local region, a pseudonym request for a local region algorithm is applied; otherwise, a pseudonym request for the inter-region algorithm is used.

Pseudonym change: For changing the vehicle's assigned pseudonym, the requested vehicle's location is rechecked. Again if the vehicle's location is in the local region, a pseudonym changing for the local region is applied; otherwise, a pseudonym changing for inter-region is used.

- *Decryption process*

In this process, for the vehicles seeking access to their real information stored on the Cloud, a request is generated and sent to the Cloud using the fog environment, as shown in Fig. 3. Vehicles have to provide their currently assigned pseudonym details along with the requested message and a key for decryption. Provided pseudonym details are checked with the records stored in the Cloud. Along with that, all the assigned pseudonyms and other related information are also authenticated. After this, a key is used along with the iwd scheme to decrypt the vehicle's encrypted information and obtain the vehicle's real information.

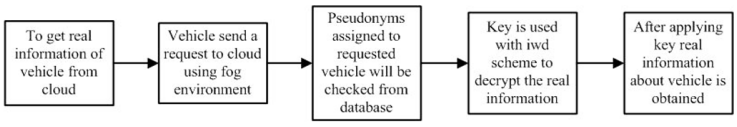

Figure 3. Decryption process for accessing real information of the vehicle.

3.3 Proposed Pseudonym Assignment and Encryption Scheme

In this scheme, local authorities of different regions have been considered. In a fog computing -supported environment, each vehicle that has been assigned a pseudonym by the local authority of one region enters the geographical region of another. Here, vehicles manage the local authorities of both regions. For safe driving on the roads, vehicle V_i periodically broadcasts safety messages and its pseudonym $\{TID_i^k\}_{k=1}^{w}$.

To implement this pseudonym-based scheme, we have proposed two mechanisms:

Pseudonym mechanism: Any vehicle can request new pseudonyms (k) on demand. Vehicles can request even 60 new pseudonyms each day. The efficient changing of pseudonyms can help in avoiding being tracked. A vehicle can change pseudonyms during driving (once every 15 minutes).

Encryption scheme: The pseudonym assignment scheme uses encryption to protect wireless communication security and exclude illegal vehicles. A.J[18], *et al.,* Debnath[19], *et al.*, Eldeen[20], *et al.* and Tandon[21], *et al.,* have used MASK as it is more secure and takes less time compared to other encryption schemes.Tandon[21], *et al.,* have used MASK with the iwd scheme for encryption. MASK, along with iwd, improves the performance of keys in terms of performance execution time. Both encryption and decryption processes take less time for encrypting and decrypting data. There is a direct substitution mapping, which results in a higher speed of conversion. AJ[18]*, et al.,* and Kumar[22], *et al.,* have applied three main steps in the MASK algorithm: matrix initialisation, key scheduling, and substitution & diffusion. Kamkar[2], *et al.,* have used an intelligent waterdrop technique with MASK, inspired by the natural water drops of a river which flows from one place to another. Here soil and velocity parameters are also considered.

Let, the soil be represented as $soil(m,n)$, and the velocity of iwd at source point be represented as $V^{iwd}(t)$.

Then, the velocity for the next node *N* can be given as:

$$V^{iwd}(t+1) = V^{iwd}(t) + x_V / (y_V + z_V . soil(m,n)) \quad (1)$$

where x_V, y_V, *and* z_V are the constant parameters for velocity.

Let the change in soil value is represented by $\Delta Soil(m,n)$ When the water drops move from position *m* to *n*, then the amount of soil that is removed is given as:

$$\Delta Soil(m,n) = x_s / (y_s + z_s . time(m,n,V^{iwd})) \quad (2)$$

where x_s, y_s, *and* z_s are the constant parameters for soil.

After the removal of soil from one location, the reduced soil is calculated as:

$$soil(m,n) = 1 - \varsigma_k . soil(m,n) \varsigma_k . \Delta soil(m,n) \quad (3)$$

where ς_k is the local soil updated parameter.

For communication of vehicle with the infrastructure, a certificate (certi) is used to authenticate vehicles' identity. Eldeen[20], *et al.,* Kumar[23], *et al.* and Tandon[24], *et al.,* have used AES and DES and also compared MASK with them. The results have shown that encryption, decryption, and certificate verification processes take less time in the MASK and iwd schemes than AES+iwd and DES+iwd. Hence, we have used the combination of MASK and iwd for encrypting the vehicle's data as it is more secure and less time-consuming when compared with the existing schemes. A vehicle uses the key and certificate ($p_u k_i$, $Cert_i$) issued by the central authority. The nearest fog node of V_i will be notified by the central authority to distribute pseudonyms to it. The central authority generates a tracking table $\left(id, p_u k_{i,} Cert_i, LT_j, \{TID_i^k\}_{k=1}^{w}, \{cert_{TIDi}{}^k\}_{k=1}^{w}\right)$ in the event database; then this tracking table is distributed to all RSUs after encryption.

4. PSEUDONYM MANAGEMENT FOR LOCAL AND INTER-REGION

If a vehicle wants to obtain the Cloud services, it has to be registered first. During the registration process, a vehicle

needs to provide all the details about its real identity. As the registration is over, the vehicle's real identity gets encrypted by implementing the proposed scheme. Now, if the vehicle requests for a pseudonym, its authenticity is checked by a certificate verification authority.

4.1 Pseudonym Requesting and Changing Algorithm for the Local Region

Vehicles requiring pseudonyms need to provide details regarding their current location, key, and certificate for verification to a local authority (LA_j). As the verification gets completed, the vehicle obtains a pseudonym, and a confirmation is sent to the LA_j that the pseudonym has been received. The local authority further updates the vehicle's pseudonym record having a pseudonym request number, certificate of currently using a pseudonym, and timestamp (t_s). If the vehicle is in coverage of LA_j, it will get a new pseudonym by utilising the corresponding key. Now, a new record of the vehicle is maintained in the tracking table of the central authority. The process for pseudonym requests in the local region is shown in Algorithm 1.

Algorithm 1: Pseudonym request for local region

1. **IF** V_i requests for pseudonym through RSU_n **DO**
2. Request for pseudonym =
   $RSU_n \| Ep_u k_i (Id\_request \| TID_i^k \| p_u k_i \| cert_i)$
   where pseudonym_request =
   $\{Vehicle\ location \| Id\ request\ number \| t_s\}$
3. **IF** TID_i^k and $p_u k_i$ is verified by LA_j and V_i lies in the range of RSU_n **DO**
4. Reply to pseudonym request =
   $Ep_u k_i \left(\{TID_i^k, cert_{TIDik}\}_{k=1}^{w} \right) \| t_s$
5. Record information in LA_j
   record = $\left(p_u k_i \| TID_i^k, cert_{TIDik}\right) \| cert_i \| t_s$
6. update information to cloud:
   Tracking_record = $Ep_u k_i \left(record \| cert_c\right) \| t_s$
7. Cloud: store and update Tracking_record of vehicle V_i
8. **ELSE**
9. No reply

If vehicle V_i wants to change its current pseudonym, a request is sent for changing the current pseudonym by the vehicle. If the vehicle is in the range of LA_j, it sends a message to the LA_j requesting for the change of pseudonym. The message sent by the vehicle contains the current holding pseudonym, certificate, key, and timestamp. First, after the verification of the vehicle, record of the concerned vehicle is updated in the database. The updated record is directly sent to the central authority of the Cloud for further updating the tracking table as maintained by the Cloud in the event storage. The process for pseudonym change in the local region is shown in Algorithm 2.

Algorithm 2: Pseudonym change request for the local region

1. **IF** vehicle V_i is in the range of RSU_n of LA_j **DO**
2. notification =
   $Ep_u k_{LAj} \left(p_u k_i \| cert_i \| TID_i^k \| cert_{TIDik} \| new\_pseudo \| t_s\right)$
   where new_pseudo = $\left(TID_i^{k+1} \| cert_{TIDik+1}\right)$
3. **IF** notification from vehicle V_i is verified in LA_j **DO**
4. update serving record in LT_j
   serving_record = $\left(p_u k_i \| TID_i^{k+1} \| cert_{TIDik+1} \| t_s\right)$
5. Reply = $p_u k_i \left(updated\ info \| cert_{LAj} \| t_s\right)$
6. update the serving information to cloud
   serving_info = $Ep_u k_{CA} \left(cert_{LAj} \| serving\_record \| t_s\right)$

4.2 Pseudonym Requesting and Changing Algorithm for Inter-region

Suppose vehicle V_i is driving to another region using the pseudonym assigned by the local authority of the local region LA_j. In that case, the vehicle has to send a request for a pseudonym to the local authority LA_p of that region, which consists of the currently used pseudonym TID_i^{z-1} of the vehicle. The pseudonym requested here will contain all the information about the concerned vehicle, i.e., request : $Ep_u k_{Lap} \left(Id\_req \| p_u k_i \| cert_i \| TID_i^{z-1} \| cert_{TiDi}^{z-1} \| t_s\right)$. Now, the local authority LA_p of the other region verifies the authenticity of the vehicle issued by the local authority LA_j. The LA_p now takes the record of that particular vehicle from the local authority LA_j and updates the vehicle's record and communicates the same with the LA_j. The LA_j now stops updating the record of that particular vehicle. The process for pseudonym requests in inter-region is shown in Algorithm 3.

Algorithm 3: Pseudonym request for inter-region

1. **IF** vehicle V_i using $TID_i^{z-1} in\ LA_p$,
2. $V_i \rightarrow LA_p$ for pseudonym request
   (pseudo request contains: information of V_i and its current id)
3. request =
   $Ep_u k_{Lap} \left(Id\_req \| p_u k_i \| cert_i \| TID_i^{z-1} \| cert_{TiDi}^{z-1} \| t_s\right)$
4. LA_p verifies V_i and LA_p terminates updating record of V_i
5. **DO**
6. LA_p reply to request
   reply = $Ep_u k_{Lap} \left(\{TID_i^k, cert_{TIDik}\}_{k=1}^{w}\right) \| t_s$
7. Record information in LA_p
   record = $\left(p_u k_i \| TID_i^k, cert_{TIDik}\right) \| cert_i \| t_s$
8. update information to cloud
   Tracking_record = $Ep_u k_i \left(record \| cert_c\right) \| t_s$
   Cloud: store and update Tracking_record of vehicle V_i
9. **ELSE**
   No reply

Suppose, vehicle V_i uses the pseudonym assigned by the LA_j in the other region of LA_p and now wants to change the current pseudonym. In that case, the vehicle sends a request to the inter-region pseudonym changing the protocol. After receiving the request for changing pseudonym, LA_p verifies the authenticity of that particular vehicle. Now, the local authority, LA_p, maintains the records and updates the same. As the verification is completed, the updated record is sent to the central authority. The process for pseudonym change in inter-region is shown in Algorithm 4.

Algorithm 4: Pseudonym change request for inter-region

1. **IF** Vehicle V_i wants to change pseudonym that is in range of LA_p **DO**
2. sends inter-region request to LA_p
3. notification=
   $Ep_uk_{LAp}(p_uk_i \| cert_i \| TID_i^k \| cert_{TIDik} \| new\_pseudo \| t_s)$
   where new_pseudo = $(TID_i^{k+1} \| cert_{TIDik+1})$
4. **IF** notification from vehicle V_i is verified in LA_p **DO**
5. update serving record in LT_j
   serving_record = $(p_uk_i \| TID_i^{k+1} \| cert_{TIDik+1} \| t_s)$
6. Reply = $p_uk_i(updated\ info \| cert_{LAp} \| t_s)$
7. update the serving information to cloud
   serving_info = $Ep_uk_{CA}(cert_{LAp} \| serving\_record \| t_s)$

5. SECURITY ANALYSIS

In this section, we have analysed the proposed scheme based on security and privacy preservation.

(a) Security requirements: The proposed scheme uses encryption and authentication mechanism, that makes it resistant to various security attacks. MASK is used for encryption, which generates encrypted information that does not depend on the characters' position in the original and encrypted information. This makes the decryption of the encrypted information very difficult. Also, the encrypted information cannot be retrieved by a brute-force attack. The usage of timestamps avoids replay attacks, and resists Sybil attacks on the proposed scheme. Vehicles change their pseudonyms without any hassle, and the previous pseudonym is removed from their memory.

(b) Privacy preservation: The location privacy of the vehicles is preserved in the proposed scheme by using pseudonyms. The vehicles can change pseudonyms once every 15 minutes, which increases the entropy of the vehicle pseudonyms. So, this reduces the chances of tracking down the location of vehicles. The increased entropy of the vehicle pseudonyms also ensures that the attacker cannot target a particular vehicle.

6. RESULTS

While executing the experiments, we have considered various scenarios for different algorithms. For a vehicle in a small region, we have used Algorithm 1 for a pseudonym request. On the other hand, Algorithm 2 has been used for changing requests for pseudonyms in the local region. If the vehicle is in a large region, then Algorithm 3 and Algorithm 4 are applied to request and change pseudonyms. There are roadside units installed at every 400 m. At the intersection, the mean value of the vehicles ranges from 40 to 130 per minute. Also, there is a traffic light at each intersection point whose red light is set for 60 sec.

Compared with Debnath[19], *et al.* and Eldeen[20], *et al,* the proposed scheme is more secure and reliable as it is resistant to many security attacks such as integrity, modification, authentication, and Sybil attacks. Further, it is efficient and faster when time parameters for the encryption, decryption, and certificate verification of the vehicle are considered. The proposed scheme time parameters have been compared with AES+iwd and DES+iwd and are shown in Fig. 4. The encryption time, decryption time, and certificate verification time for our proposed scheme are 1.74 ms, 0.83 ms, and 5.2 ms. Pseudonym allocation, generation, and total time are taken for local and inter-region is calculated. Their graphical representation is shown in Figs. 5 and 6. It can be seen that the time taken for a change of pseudonym is more when compared with pseudonym requests for both local and inter-region. This is because the requesting vehicle will be first verified in pseudonym change, and its previous pseudonym history will be checked. If it satisfies all the conditions, then the changing request will be processed.

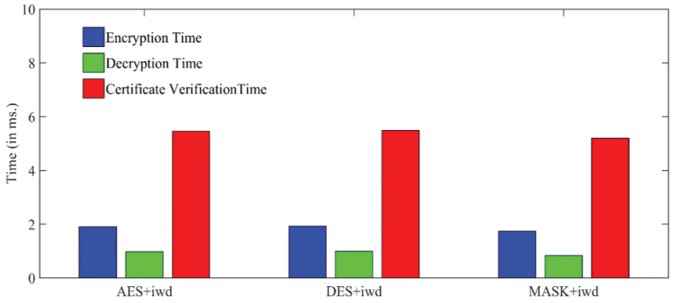

Figure 4. Comparison of MASK+iwd with AES+iwd and DES+iwd.

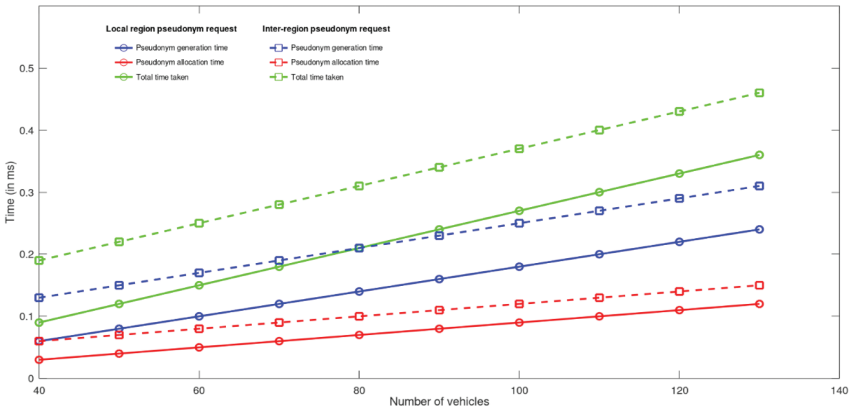

Figure 5. Pseudonym requesting for local region and inter-region.

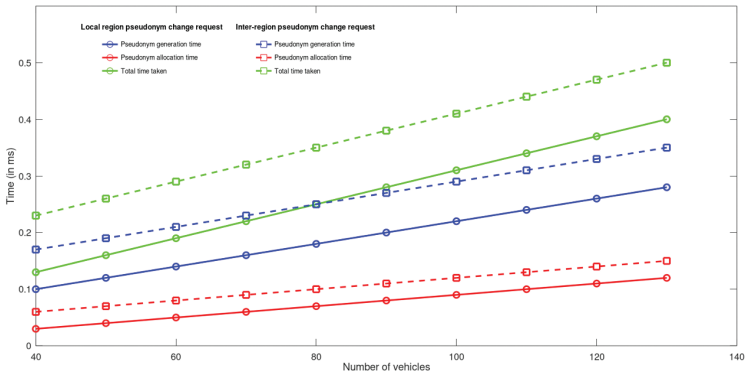

Figure 6. Pseudonym changing request for local region and inter-region.

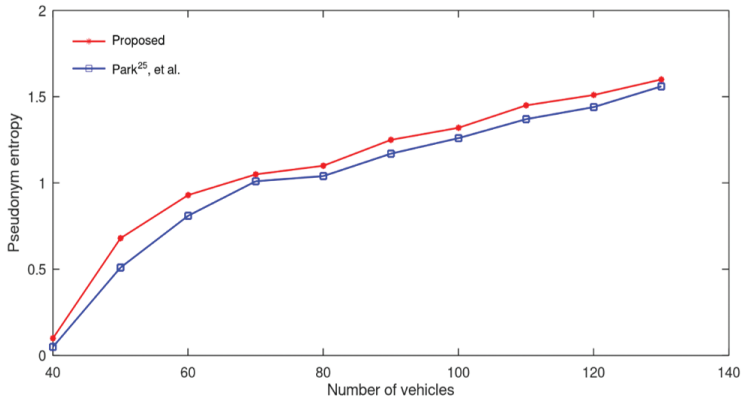

Figure 7. Pseudonym entropy comparison of the proposed scheme with the existing scheme.

In Fig. 7, the graphical comparison of pseudonym entropy for the different numbers of vehicles is shown. It is observed that the proposed scheme has the higher pseudonym entropy and hence less prone to attackers.

7. CONCLUSIONS

This paper has implemented a hybrid security scheme of swarm intelligence consisting of MASK and iwd scheme to encrypt the military vehicle data with pseudonym assignment to ensure security and protection to their location and movement-related privacy. Implementation of pseudonyms helps in further enhancing the safety of the military vehicle. The proposed framework for vehicle-to-vehicle communication uses fog computing to the edge of the network. The implemented security scheme assures the privacy preservation of the data of military vehicle against security attacks. Also, this scheme is efficient in terms of encryption and decryption of the data. By using this scheme, location, and movement privacy of the vehicle can also be improved. In the future, we will try to implement our scheme for more defence vehicles such as armoured vehicles, aerial vehicles, un-manned group vehicles, and or any vehicles that require a high degree of privacy.

REFERENCES

1. Chaurasia, B.K.; Verma, S.; Tomar, G.S. & Abraham, A. Optimilabelled pseudonym updation in vehicular ad-hoc networks. *Trans. Comput. Sci. IV* Springer, Berlin, Heidelberg, 2009,136-148. doi: 10.1007/978-3-642-01004-0_8
2. Kamkar, I.; Akbarzadeh-T, M.R. & Yaghoobi, M. Intelligent water drops a new optimisation algorithm for solving the vehicle routing problem, *In proc. of IEEE International Conference on Systems Man and Cybernetics (SMC)*, 2009, 4142-4146. doi: 10.1109/ICSMC.2010.5642405
3. Shah-Hosseini, H. The intelligent water drops algorithm: a nature-inspired swarm-based optimisation algorithm, *International Journal of Bio-Inspired Computation*, 2009, **1**(2), 71-79. doi: 10.1504/IJBIC.2009.022775
4. Papadimitratos, P.; Buttyan, L.; Holczer, T.; Schoch, E.; Freudiger, J.; Raya, M.; Ma, Z.; Kargl, F.; Kung, A; & Hubaux, J.P. Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*, 2008, **46**(11), 100-109. doi: 10.1109/MCOM.2008.4689252
5. Eichler, S. Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility. *In* IEEE Intelligent Vehicles Symposium (IV '07), June 2007. doi: 10.1109/IVS.2007.4290171
6. Petit, J.; Schaub, F.; Feiri, M. & Kargl, F. Pseudonym schemes in vehicular networks: A survey. *IEEE communications surveys & tutorials*, 2014, **17**(1), 228-255. doi: 10.1109/COMST.2014.2345420
7. Kang, J.; Yu, R.; Huang, X; & Zhang, Y. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 2017, **19**(8), 2627-2637. doi: 10.1109/TITS.2017.2764095
8. Xiong, H.; Hou, Y.; Huang, X. & Zhao, Y. Secure message classification services through identity-based signcryption with equality test towards the Internet of vehicles. *Vehicular Communications*, 2020,100264. doi: 10.1016/j.vehcom.2020.100264
9. Kumar, G.; Rai, M.; Saha, R.; Buchanan, W.J.; Thomas, R.; Geetha, G.; Kim, T.H. & Rodrigues, J. A Privacy-Preserving Secure Framework for Electric Vehicles in IoT using Matching Market and Signcryption. *IEEE Transactions on Vehicular Technology*, 2020. doi: 10.1109/TVT.2020.2989817
10. Jiang, S.; Zhu, X. & Wang, L. An efficient anonymous batch authentication scheme based on HMAC for VANETs. *IEEE Transactions on Intelligent Transportation Systems, 2016,* **17**(8), 2193-2204. doi: 10.1109/TITS.2016.2517603
11. Groza, B.; Andreica, T.; Berdich, A.; Murvay, P.S. & Gurban, E.H. PRESTvO: PRivacy Enabled Smartphone Based Access to Vehicle On-Board Units. *IEEE Access*, 2020, **8**, 119105-119122. doi: 10.1109/ACCESS.2020.3003574
12. Safavat, S. & Rawat, D.B. On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart

Cities. *IEEE Transactions on Intelligent Transportation Systems*, 2020
doi: 10.1109/TITS.2020.3008361

13. Jing, T.; Pei, Y.; Zhang, B.; Hu, C.; Huo, Y.; Li, H. & Lu, Y. An efficient anonymous batch authentication scheme based on priority and cooperation for VANETs. *EURASIP Journal on Wireless Communications and Networking*, 2018, **2018**(1), 1-13.
doi: 10.1186/s13638-018-1294-z
14. Huang, J.L.; Yeh, L.Y. & Chien, H.Y. ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.,* 2011, **60**(1), 248–262.
doi: 10.1109/TVT.2010.2089544
15. Lo, N.W. & Tsai, J.L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Transactions on Intelligent Transportation Systems,* 2015, **17**(5), 1319-1328.
doi: 10.1109/TITS.2015.2502322
16. Zhang, J.; Zhong, H.; Cui, J.; Xu, Y. & Liu, L. An Extensible and Effective Anonymous Batch Authentication Scheme for Smart Vehicular Networks. *IEEE Internet of Things Journal*, 2020, **7**(4), 3462-3473.
doi: 10.1109/JIOT.2020.2970092
17. Wang, S.; Mao, K.; Zhan, F. & Liu, D. Hybrid conditional privacy-preserving authentication scheme for VANETs. *Peer-to-Peer Networking and Applications*, 2020, 1-16.
doi: 10.1007/s12083-020-00916-3
18. AJ, P.; Paul, V. & Mythili, P. Matrix Array Symmetric-Key Encryption. *Journal of the CSI, 2007,* **37**(1).
19. Debnath, D.; Deb, S. & Kar, N. An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher RGB Image Steganography. *In Proc. of International Conference on Computational Intelligence and Networks (CINE),*2015, 178-183.
doi: 10.1109/CINE.2015.41
20. Eldeen, M.A.S.; Elkouny, A.A. & Elramly, S. DES algorithm security fortification using Elliptic Curve Cryptography. *In* 2015 Tenth International Conference on Computer Engineering & Systems (ICCES), 2015, 335-340.
doi: 10.1109/ICCES.2015.7393071
21. Tandon, R. & Gupta, P.K. A Novel and Secure Hybrid iWD-MASK Algorithm for Enhanced Image Security. *Recent Patents on Computer Science*, 2019, **12**, 1-11.
doi: 10.2174/2213275912666190419214900
22. Kumar, T. & Chauhan, S. Image Cryptography with Matrix Array Symmetric Key using Chaos based Approach. *International Journal of Computer Network and Information Security,* 2018, **3,** 60-66.
doi: 10.5815/ijcnis.2018.03.07
23. Kumar, P. & Rana, S.B. Development of modified AES algorithm for data security. *Optik-International Journal for Light and Electron Optics,* 2016, **127**(4), 2341-2345.
doi: 10.1016/j.ijleo.2015.11.188
24. Tandon, R. & Kundra, S. Image Security with Advanced Encryption Standard Using Swarm Intelligence Technique. *International Journal of Advances in Science and Technology (IJAST),* 2015, **3**(3), 1-10.
25. Park, Y.; Sur, C. & Rhee, K.H. Pseudonymous authentication for secure V2I services in cloud-based vehicular networks. *Journal of Ambient Intelligence and Humanized Computing*, 2016, **7**(5), 661-671.
doi: 10.1007/s12652-015-0309-4

CONTRIBUTORS

Ms Righa Tandon is currently pursuing a PhD degree from the Jaypee University of Information Technology in the Department of Computer Science and Engineering. She is an IEEE member with a key interest in Information Security, Fog Computing, Image Processing, Network Security and Predictive Computing.
She has carried out the formulation of the problem statement for the study, the survey of existing literature in similar work, an overall analysis of the work, and formulation of results and the implementation of the algorithms.

Dr P.K. Gupta is currently working as an Associate Professor in the Department of Computer Science and Engineering at Jaypee University of Information Technology (JUIT). He has extensive research experience in Internet-of-Things, Information security, Cloud Computing, Machine learning, and Deep Learning. He has authored more than fifty research papers in the peer-reviewed international journals and conferences and edited more than 10+ books with reputed publishers like Springer, IGI Global USA, IEEE USA, etc.
He has provided valuable inputs towards the overall aim and objectives of the work, designing of methodology, implementation, and the validation of the results.