Secure VANETs: Trusted Communication Scheme between Vehicles and Infrastructure Based on Fog Computing

Muhammad ARIF[1], **Guojun WANG**[1]*, **Valentina Emilia BALAS**[2]

[1] Department of Computer Science and Technology, Guangzhou University, Guangzhou, Guangdong, 510006, China
[2] Aurel Vlaicu University of Arad, Romania
arifmuhamamd36@hotmail.com, balas@drbalas.ro
csgjwang@gzhu.edu.cn (**Corresponding author*)

Abstract: In the Vehicular Ad-hoc Networks (VANETs), a vehicle or the vehicle driver could be recognized and tracked by eavesdropping its queries (e.g., beacons) by an adversary as these contains personal information like location, speed, and communication of the vehicles. This attack leads to threats to the vehicle`s location and leakage of personal information. The current solution, is to use the anonymizer as a third trusted party between the vehicles and the LBS. In this paper we refer to the use of a Fog server with Fog anonymizer to secure the communication among the vehicles and LBS. Our scheme consists of four phases. In first phase, the vehicle driver initiates the communication process and generate the encrypted messages. These messages may contain the sub-messages. In phase 2, the Fog server received the messages via different roots. The *Fs* combined the messages and decrypt the messages based on the PK received by the vehicle. All the Fog server perform the same task for encryption and decryption. If any of the Fog server was compromised, we still had the link for communication. In Phase 3, the Fog anonymizer receive the messages from the Fog node, anonymize them based on the anonymization process. Thereafter, the Fog anonymizer send these messages to LBS to achieve desired goals. The Fog anonymizer perform the same job for anonymization and de-anonymization, while sending and receiving the messages from the LBS. In the last phase, the LBS received the messages from the Fog anonymizer, understand the communication messages, compile the desired results, and sent them back to the Fog anonymizer. Our analysis shows that the proposed scheme preserved the location privacy based on the queries at low communication and computational cost.

Keywords: Privacy, Vehicles, Communication, Infrastructure, RSU, OBU, Encryption, Decryption, Message, Location.

1. Introduction

In the coming years, VANETs will perform a significant role in enhancing road security, safety and the traffic efficiency in transportation systems [1]. The technology offers a variety of interesting applications, which include security plans such as alerts and emergency reports for non-security applications e.g., entertainment, environment, and weather [2]. Many security applications claim to rely on a basic mechanism, which means that vehicles continuously transmit security messages [3], [4,16]. These safety messages contain the knowledge about the present status of the vehicles, such as the speed, direction, position and acceleration [5,35].

Security and privacy are one of the main challenges in VANETs. Security messages must be approved to avoid security attacks [6-10, 29-30], such as the addition of false data, the modification of published messages and the reproduction of attacks [7]. These attacks can cause serious damage to the VANETs system [7]. In fact, as long as the wireless media in VANETs broadcast the unencrypted messages. A passive opposition can be easily controlled in all broadcast messages and can be controlled by the places explored by focusing on the vehicles over a period of time [8]. This leads to the privacy of drivers, since there is usually a strong relationship between a vehicle and its driver [9].

When it comes to urban areas, the situation gets worse. Because these areas are often known by the presence of many IDPs, such as hospitals and restaurants, recognizing the driver's position can lead to the disclosure of vital information about their lives. This can cause the driver many problems, such as the disclosure of information on the number of the driver`s hospital visits to his employee [10]. Therefore, the protection of confidential privacy is important, since lack of protection can prevent the use of VANETs technology [11].

Wu et al. [12] and Zhang et al. [13] came up with a CPPA strategy based on the group signature in which the OBUs did not need to store the private data. The TA can adequately identify the adversaries based on the cancellation list without wasting the cost that incur during retrieval of list. However, repudiation changes quickly due to fast vehicle speed and network topology. As the vehicle progresses, the problem of updating and choosing group managers and members becomes dynamic. Chim et al. [14] proposed a project using a two-way communication operation,

https://doi.org/10.24846/v27i2y201811

in which the RSU used a pseudo identification to secure its true identity when communicating messages by creating a common key in the RSU manipulation phase and TA, where the TA can also see the true identity behind the quasi-identity. In the certification phase, RSU issues a notification message with a Bloom filter to reduce the cost of OBU calculations, but Horng et al. [15] later noted the proposed approach by Chim et al. [14] cannot resist tampering attacks; thus, malignant vehicles can exchange themselves as legal means to send malignant messages after stopping a legal message. However, Lee et al. [18] later pointed that this plan cannot achieve undeniable performance, Liu et al. [19] noted that the plan could not change resistance to an attack for improving the competence of communication, while providing the conditional privacy of the vehicles in the VANETs.

A typical VANETs includes registration permissions, administrative applications and servers, location based services, proxy servers, vehicles, RSUs, OBUs, group leader (depending on model) [20-24], multimedia service provider, and transportation center for public and private companies as show in the Fig. 2. New features in the vehicles includes event recording (*EDR*), *GPS* receiver and front and rear radars to detect obstacles [24-28, 34]. Communications through VANETs can be used to track vehicle locations. There are three types of communication in the VANETs V2V, V2I, and Inter road side communication (IRs) as shown in the Fig. 1.

To address the aforementioned issues we proposed a technique in which we provide the query-based location and communication privacy in V2I and V2V. For this purpose we used Fog server and Fog anonymizer. We provide twofold step privacy to the vehicle drivers, so the adversaries cannot track the vehicle real location as well as the vehicle communication.

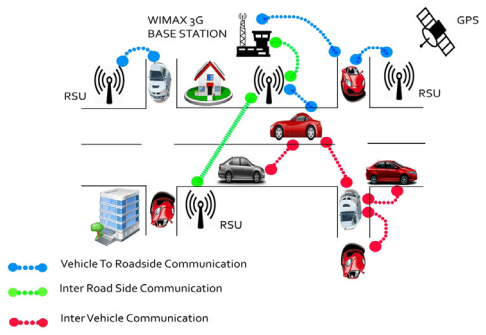

Figure 1. Communication Process in the VANETs

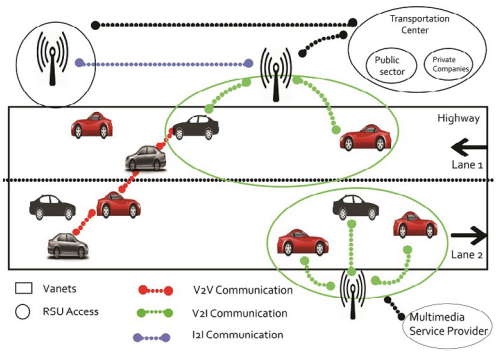

Figure 2. VANETs Configuration

3. Proposed Methodology

The proposed mechanism is based on the k-anonymity and the multi-path based communications among the V2V and V2I to give the senders k-anonymity at the VANETs level.

3.1 Sender k-anonymity

Let M be a communication query created by a vehicle v, and have the *k-anonymity* where k is a privacy reference for vehicle v, if the probability of combining the v as the query of sender is less or equal to $1=k$. In the forthcoming section, we present how the k-anonymous query based communication is achieved and broadcast by the vehicle in VANETs by RSUs and OBUs to *Fs*. How the Fog anonymizer receives the queries from the *Fs* and forwards them to the LBS and after receiving the acknowledgment from the LBS, how it sends them back to the *Fs*, where *Fs* sends the queries to the vehicle v. And how these queries can only be decoded by the desired vehicle who initiated the query covered from the auxiliary k - 1 vehicles, to assure the senders *k-anonymity* against the attackers including the LBS.

3.2 Overview of the system

Let V, N, *Fs* and LBS be the set of vehicles, network, Fog server and location-based server respectively. In our system vehicle is the entity that submits the communication query, the server is the network that provide the communication among the vehicles. Fog server *Fs* is the extra layer between vehicles and the Fog anonymizer provide the security and privacy for the communication. Fog anonymizer provides the trusted communication between the vehicles and the location-based servers. Our scheme mainly consists of four phases as shown in Fig.3.

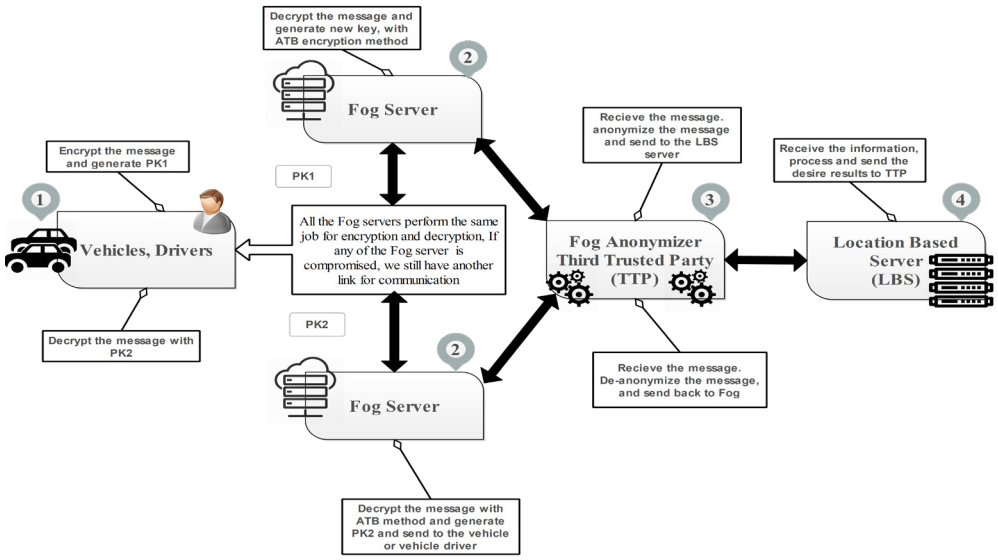

Figure 3. Overview of the Proposed Work

Phase I. In this phase vehicle driver initiates the communication process and generate the messages *M*. This message *M* may contain the sub-messages {*M*=*m*1,*m2,...,mk*}. After initiating the communication process the vehicle driver *v* encrypt the message and generate parent key (*PK*1) based on *ATB* encryption.

Phase II. In this phase, the *Fs* receive the messages *{M = m*1*, m*2*, ..., mk}* via different roots. Then it combines and decrypt the messages based on the PK received by the vehicle *v*. All the *Fs* perform the same task for encryption and decryption. If any of the *Fs* compromised, we still have another link for communication.

Phase III. In this Phase the third trusted party (TTP) works as Fog anonymizer and receives the messages from the *Fs* node. Anonymize the message based on the anonymization process and send to the LBS for the results. The Fog anonymizer perform the same job for anonymization and de-anonymization, while sending and receiving the messages from the LBS.

Phase IV. At the end, LBS understand the communication messages, compile the desired results that were received from Fog anonymizer and send them back to it.

3.3 Fog computing

Recently, fog computing has become an active cloud-related research area. It was incorporated by Cisco in 2012 [31]. It is an extended paradigm of cloud computing where network edge is employed for data processing and services contrary to the existing technique in which this is completely done in the cloud. It offers many advantages in comparison with traditional systems as location awareness, mobility support and low latency can be achieved by using fog architecture which eventually places the fog nodes closer to end-users. Fog computing also incorporates core cloud services. It changes conventional data centers into heterogeneous and distributed platforms as well. Therefore, fog computing supports the applications of internet of things in vehicular networks, actor/sensor networks and industrial automation that require the processing of context awareness and sensitive delays [32].

3.4 Fog Server Fs

Fs acts as intermediate tier between the vehicles and Fog anonymizer to provide the secure transmission of communication in VANETs. So, first of all Fog server *Fs* decrypts the message *Mv* with the secret key *PK* shared through *v*, then it transmits it to the Fog anonymizer. Fog server *Fs* confides on wireless network *N* to handle the messages mobility and delivery of the *PK*. Despite the fact that all the vehicles receive the message`s, vehicle *v* is the single vehicle with the secret key *PK*. And thus, it is the only vehicle that can decrypt the response and avail the service of VANETs. On the contrary, others did not have the vehicle *PK*, so they deleted the messages.

3.5 Privacy in Fog Computing

The most concerning problem of the user is the risk of privacy leakage in VANETs. In fog computing, the algorithms of privacy preserving are run among the fog nodes and the cloud, because there is no problem of computation, processing, and storage for the both sides, and these are sufficient. And the running algorithms are resource prohibited at end device, they usually collect the data for the end devices as shown in Fig. 4, for the privacy preservation at the fog nodes the homomorphic encryption is used for the preservation of the privacy without the decryption. For the statistical and aggregation differential privacy is applied to validation of non-exposure of privacy of an arbitrary and conflicting single entrance in data set.

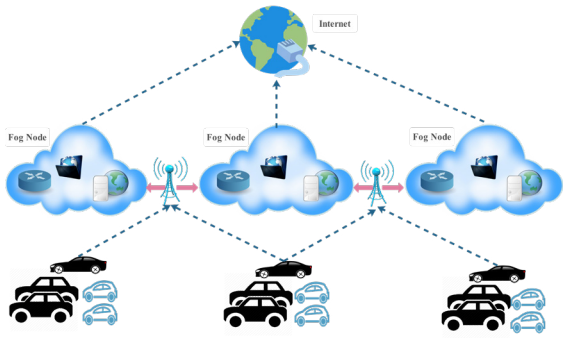

Figure 4. Communication through Fog Nodes

3.6 Third Trusted Party Architecture (Fog anonymizer)

The Fog anonymizer, acts as an intermediate tier between the vehicle and the LBS as shown in Fig. 5. In this paper we use CASPER as a Fog anonymizer architecture. This architecture is a centralized trusted entity which is responsible for gathering and providing the required privacy for each vehicle in the network. Fog anonymizer received the exact message from the vehicle`s and blurs the information and send to the location based server. It also provide powerful privacy guarantee with high quality services. The four factors we have recognized for abstaining the shortcomings of the previous location Anonymizer are; quality, accuracy, flexibility and efficiency [25-30]. Minimum spatial area requirements and k anonymity has been supported by Casper [33]. The approach in which user's privacy could be adjusted depending upon the user`s needs. Complete pyramid and imperfect pyramid are the types of pyramid structures, subsumed by the Casper to deal with systems scalability.

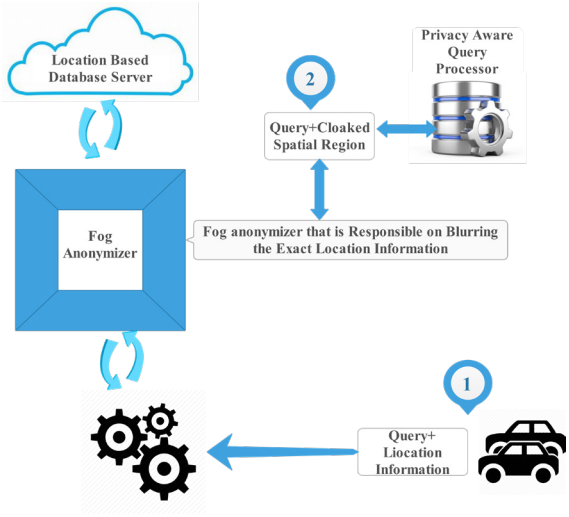

Figure 5. Fog Anonymizer Architecture

3.7 Anonymous Request

The anonymous inquiry process is generated by the vehicle or vehicle driver *v*, which intends to approach the applications mentioned earlier, provided by the LBS. There is no communication overhead for the *V* in execution of inquired queries for communication process, *v* commitments to first define the *M* message and the privacy preferences *k*. Then, *v* engenders the message identity *mid* and transmits the message *M* into the *k* data movement generating the messages *{m*1,*m*2,..*mk}* and *PK*. Derived messages are disseminated between neighbor's vehicles in the VANETs and PK forwarded to the Fog server through RSU.

Distinctive methods (based on the networks state or the vehicle positions) can be implemented for the broadcasting of messages in the vehicles. Our method consists in using a simple approach for the distribution of messages among the vehicles in *v*s communications range. Our broadcasting method works as follows. Inquired vehicle *v* encrypts every message *mi* using ABE method and generate *PK* shared among vehicle`s *Vs* and Fog server *Fs,* that is *{mi = {(ABE)PK(mi)||mid}}* for every *{i* = 1, *k}*. The existence of message *M,* identity *mid* in all messages allows the vehicles to categorize dissimilar sub-messages associated to the same message *M*. Requester *v* then randomly choses *k* -1 vehicle`s *Vs* in his communications range, and send the messages from *{m*1 → *mk}* to each of them. It then sends these messages to Fog server via wireless networks *N*.

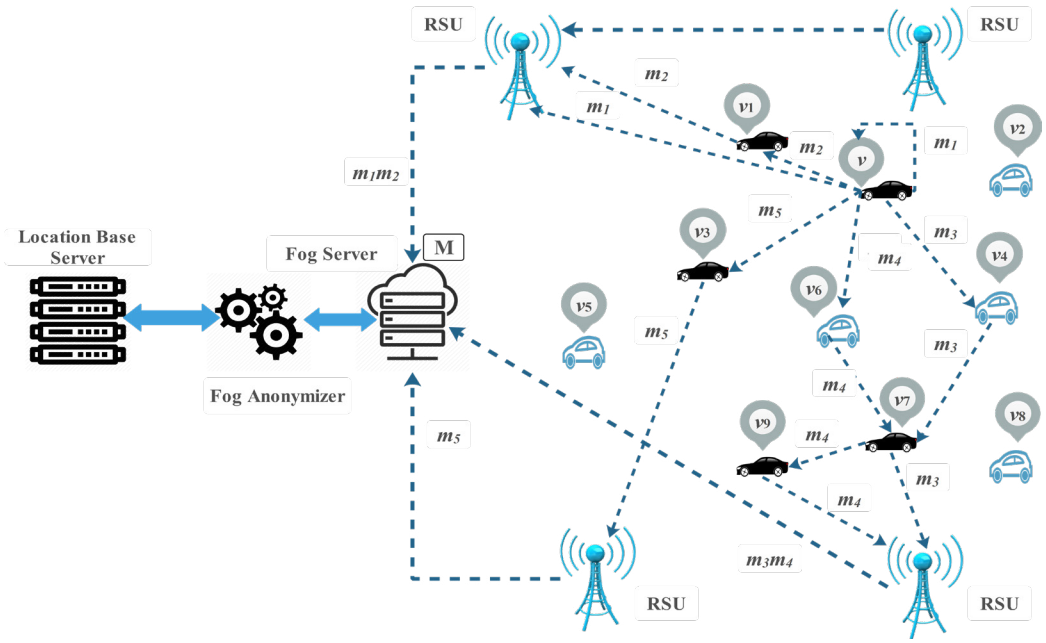

Figure 6. Anonymous Request Process

Upon accepting the messages *mi* from every vehicle in the communication range then vehicle *v*1 first checks the *mid*. If it is already acknowledged to send the message with same *mid*, *{mid Є Sent}*, vehicle *v*1 transmits *mi* to next vehicle *v*2 in the communications range. On the other hand, it randomly choses, with the probability *{vf* = 1=2*}*, either to transmit *mi* to the next vehicle *v* in the communications range, or to send this *mi* without the *mid* to the Fog server *Fs*.

After the transmission process each selected vehicle *v* separately sends the messages received by *Fs*. These messages from all the vehicles are forwarded to *Fs* through RSUs. Now *Fs* can decrypt each message incrementally through *PK*, reconstruct the messages and send them to the Fog anonymizer. The Fog anonymizer ammonize the message and send to the LBS for the desired outcomes. Fig. 6 illustrates an example of the anonymous request generation process where, blue vehicles transmit a message to the next vehicle, while the black vehicles send a message to the Fog server *Fs* through *RSU*. The message generator vehicle *v* describes $k = 5$ and distributes the message *M* in five sub-messages *{m*1*, ..., m5}*. Messages are then encrypted with the ABE method and shared between vehicle`s *{vs= v, ... ,vk}* and Fog server *Fs*, and *mid* is appended with each of the sub-messages. And the *PK* shared with Fs through *RSU*. The inquired vehicle *v* sends message *m*1 to *Fs* and transmits the other *{k* – 1*}* messages to vehicles in the communications range. Categorically, messages *m*2 and *m5* are broadcast to the vehicles *v*1 and *v*3 that transmits them to the *Fs*. Considering *v*4 does not accept to transmit *m*3, message *m*3 then gets a forwarded path {*v*4 → *v*7}. Message *m*4 gets a forwarded path {*v*6 →*v*7 → *v*9} because, when the message is acknowledged by *v*7 and *v*7 considers that it has already got a message (*m*3) with the same *mid*, and then transmits to {*m*4 → *v*9}. Finally, vehicle`s {*v, v*1*, v*3*, v*7, and *v*9} send a message to *Fs* via *N*.

3.8 Cloaking Algorithm (Fog Anonymizer)

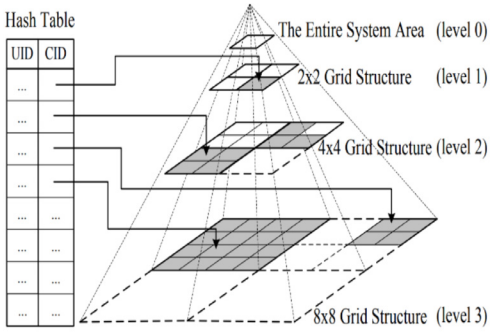

Figure 7. CASPER Anonymizer Structure

A top-down optimization algorithm is utilized by the Casper [33], he the generic pyramid data structure illustrated in the Fig: 7, begins from a cell that allocates the vehicles at lowermost level, then the suitable private cell is figured out by devastating the pyramid structure. In cell splitting

operations, a cell at level i should be divided into four levels at level i+1 if at least one user is in *cid* with a private profile that can be satisfied by some cells at i + 1 level. In order to maintain the aforesaid criterion, Casper makes the user v_r suitable for every cell. If the new element v_{new} to the cell *cid* has more relaxed privacy requirement than *ur*, the division of the *cid* cell into four cells at the i + 1 level leads to having a new cell that will have the privacy requirements which satisfy the v_{new}. In such situations, *cid* will be broken down by the split cell algorithm and its contents will be distributed among all the new cells. Adversely, only v_r will be amended.

Necessarily, only v_r will be updated by the algorithms in the case, if any of the users send back the code. If the users in the *i-level* cell are subject to difficult rules that cannot be satisfied at the *ith* level, the four cells at Level *I* that is higher than *i*-1 will be integrated into one cell. The four cells of the surface *i* will be held together by the algorithm for the assistance of the vehicle. If the corresponding user quits these cells, an inspection is made by the algorithms in order to assure that they require cell at level *i*. The four cells are integrated to their original cell by the algorithm, in case if there is no urgency of any cell at level *i*. Subject to the fresh entry of the user in the cells of level *i*, only the related data to will be updated. The *K – anonymity* along with the minimum spatial requirements is also backed by this algorithm.

Prominently, the concept is that ahead of application for any location-based service, a batch of the peers of the vehicle driver should be created either through single-hop or multi-hop communication. Later on, the existing space is computed as the region that encompasses the whole peer group. The user desires for the nearby gas station whilst all five are anonymous.

Conceptually the user is unidentifiable among the five users. Henceforth, the user must collaborate with the other four neighbors acting as a group. Thereupon, the user allots his accurate location within the area that encompasses the whole group of the vehicles {*v; v*1*; v*3*; v*7*; v*9}. The vehicle or vehicle driver randomly appoints another member of his group acting as an agent. After getting the desired results from the LBS, Fog anonymizer again encrypt the message with ABE encryption method that is *{Mr={(ABE)PK(Mr)||v}}*, also generate new *PK* and shared with the vehicle *v* through *RSU*.

3.9 Anonymous response

In our scheme the response is anonymous because no one can know about the queries and communication. If in the case that the LBS is compromised no one can track the location, query, as well as the communication, because the LBS did not know the exact query or location of the vehicle or vehicle driver. Fig. 8 represents an illustration of anonymous feedback to the query in Fig. 8. Encrypted Queries *Mr* are broadcast

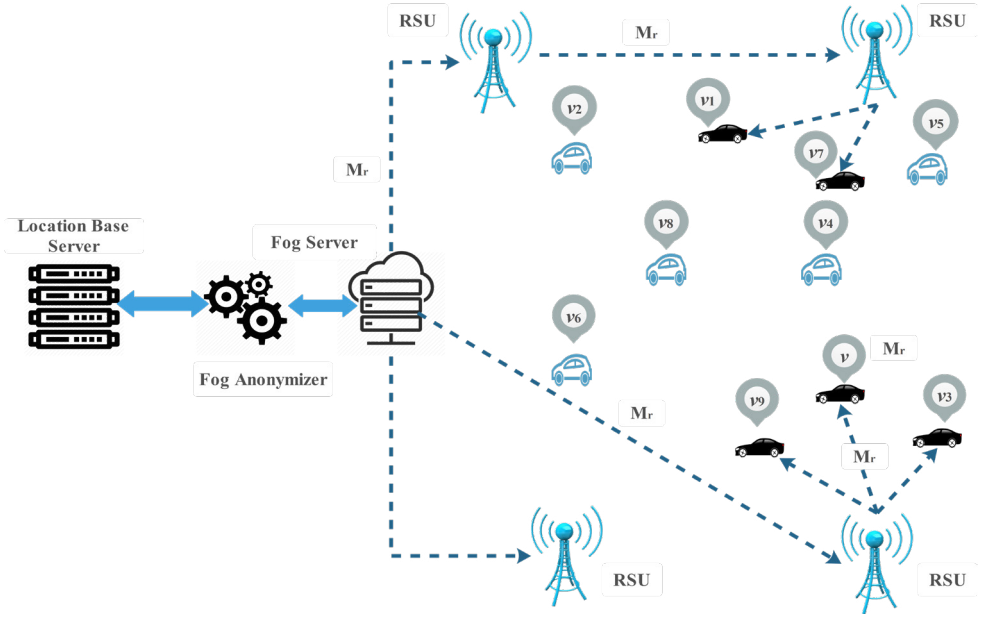

Figure 8. Anonymous Response Process

to all the vehicles utilized in Fig. 8, that are, *{v, v1, v3, v7, v9}*. When *v* collects the message, and decrypt it with the key *PK* shared by Fog server *Fs*. The auxiliary vehicles deleted this message *Mr*, because they do not have the key.

4. Analysis and Discussion

4.1 Security Analysis

Our secure communication methods provide full privacy preservation for both vehicle-wise and server wise and the privacy for the vehicles in terms of both unlink-ability and anonymity. Our analysis will focus on how this plan can maintain the vehicle`s location and privacy communications and resist the potential privacy leak through the anonymizer and other individuals in the vehicle`s network. To examine the vehicle-wise privacy, by our proposed method, a vehicle always self-generates a new key for its messages when establishing a new communication session with the server. So, it is computationally impossible for a vehicle or a group of vehicles to notice the real identification of others vehicles.

In connection with V2I and V2V, the LBS does not notice the location and communication information about the vehicle or the vehicle driver. Since the spatial area is a cloaking area of the *K* vehicles, the LBS cannot accurately locate every vehicle with a probability greater than 1=*K* because of the *K*'s anonymity principle. The results of the demands generated by the LBS are the candidate outcomes for all vehicle and vehicle drivers in the area. These results are anonymous for the adversaries and the LBS because of the encryption and anonymization process. Therefore, they cannot obtain location information about the vehicle or the vehicle driver. The Fog anonymizer cannot know every vehicle actual location because we already perform the encryption through vehicle drivers and *Fs*. The location and the communication information from each vehicle into a Fog anonymizer, are encrypted locations. The decryption function parameter is known only by vehicle`s (*vs)* and *Fs*.

The vehicle driver does not know the location of another vehicle during communication along with the LBS, using the RSU. Fog anonymizer can correctly capture the results of each vehicle or vehicle drivers, and send them back to the latter one, every vehicle or vehicle driver get their own results of their queries without knowing the information about others. Even if a small number of mischievous vehicles collaborate, they cannot understand the other concerns of truthful vehicles or vehicle drivers. As for the *Fs* server, it has the key *PK* generated by the *v* to decrypt the message *mid*, and hence it knows the real identification of the *v* who agrees to submit the communication query. In case that the *mid*, the *PK* and the renewal time is randomized, and all the *mids* have the same acceptable time duration, *Fs* link the relevant *mids* and *PK* to the related vehicle *v*. And the LBS server, since it does not handle any communication inquiries that consists of *mids* at the time of the authentication and communication stage, it does not have any information about which vehicle *v* is sending the communication inquiry. So, our method prevents and hinders the vehicular communication from tracing the communication as well as the location of the vehicles.

4.2 Simulation

We tested our design using the Veins1 simulation environment, based on two sets of simulation tools, both of which are well-designed in the corresponding domain. Extensive traffic mobility models, especially with regard to intersection management, are provided by SUMO. The main parameters for the evaluation are given in the Table 1.

Table 1. Description of the parameters

Parameter	Value
Simulation framework	OMNet++, Sumo and Veins
Area	100 KM2
Vehicles	100-200
No of RSU	25
Transport Protocol	UDP
Propagation model	Nakagami
Speed	15,20,25,30 m/s
Maximum acceleration	6 m/s
Maximum deceleration	4 m/s
Channel bandwidth	12 MHz
OBU receiver sensitivity	-80.0 dBm
Antenna height	1-1.5 m
Types of antenna	Omnidirectional
Transmission range	500 m
Anonymity level	2,3,4,5
ROI size	9 km^2
Network layer	802.11p and IEEE 1609.4

4.3 Evaluation

In this unit, the performance and adaptability of our proposed system under different system conditions are examined. We executed the experiments concentrating on performance of our scheme.

4.4 Performance Analysis

There are four entities in our proposed scheme, and we calculate the cost of computation of these four entities, the running time of the vehicle is $O\ (N + mk)$, where N, m, and k are the vehicles, messages, and anonymity level respectively. The running time of the Fs is $O\ (N + m)$, where N is the number of the vehicle and m is the number of the messages, because Fs is only responsible to collect the messages from the vehicle encrypt and forward them to the Fog anonymizer. The running time of the Fog anonymizer is $O\ (KY * NZ)$, where the Y and Z are the constants, k, and N are the anonymity level and vehicles respectively. The complexity of the LBS is $O\ (N + logm + mr)$, where N are vehicles and m are messages and r are the required results. So, the total complexity of system is given below.

$$O\ (N + mk + N + m + K_X * N_Y + N + Logm + mk) \quad O\ (3N + 2mk + logm + K_X * N_Y)$$

We excluded the constant, so the final computational cost is given below.

$$O\ (N + mk + logm + K_X * N_Y)$$

The computational cost between the vehicle to vehicle communication is $O\ (N+logm)$ where m are queries among the vehicle`s communication. We express its communication as O (C), where C is used as constant. Similarly to the communication of the vehicle and the Fs, then, we will consider the communication cost between the Fs and the Fog anonymizer. The communication cost among the vehicles and the Fs becomes $O\ (Ck + D)$, where C and D are the constants, and we reduce it as $O\ (k)$. The communication cost between the $F\ s$ and the Fog anonymizer is $O\ (Ak + B)$. Lastly, we examine the communication cost between the Anonymizer and the LBS. So, the communication cost is $O\ (KC * mD)$, where C and D are the constants. So the total cost among the vehicles and LBS is $O\ (k + KA * mB)$. The cost between the vehicle to vehicle communication is the process time of the cloaking method which is associated to the degree of anonymization k and the number of vehicles N, so the computational complexity is $O\ (KM * mN)$, where M and N are constants. So in simple, the computational complexity is $O\ (K * m)$. The time complexity of any Anonymizer mainly depends on its clocking algorithm. To calculate the time complexity and the communication cost (CC) of the scheme, we run the simulations. Fig. 9 (a, b) represents the processing time of the scheme at different stages. They contain the vehicles information on X-axis and the time on Y-axis.

Fig. 9 (a, b) show the vehicle processing time. For this purpose we simulate 100 vehicles and it is clearly shown that the processing time is very low. Fig. 9 (a and b) represents the processing time from Vehicles to Fog anonymizer and from Fog anonymizer to LBS respectively, same simulation has been done for this experiment and the processing time is also very low.

The communication cost (CC) of the scheme at different stages is shown in the Fig. 9 (c, d). They contain the Vehicle information on the X-axis and memory on the Y-axis. Fig. 9 (c, d) shows the CC of the vehicles when they start communicating through Fog anonymizer with the RSU or with other vehicles in the group. Fig. 9 (c) show the CC from Fog anonymizer to the LBS. the results shows that our proposed scheme have very low CC. Fig. 9 (d) shows the CC about V2V, and V2I communication from fog anonymizer to LBS.

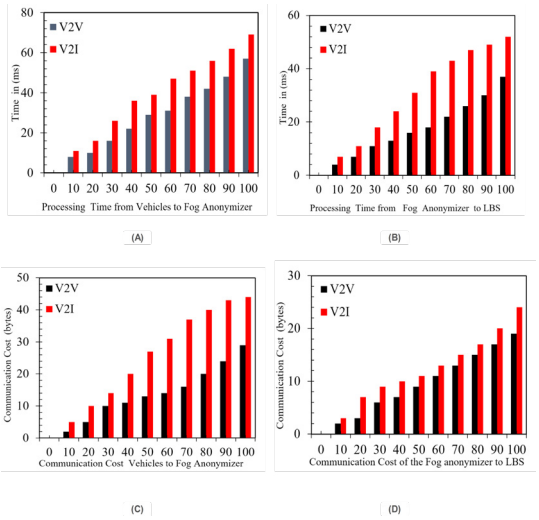

Figure 9. (a) Processing Time of Vehicles to Fog anonymizer,(b) Processing Time from Fog anonymizer to LBS, (c) Communication Cost of the Vehicles to Fog anonymizer, (d) Communication Cost from Fog anonymizer to LBS

4.5 Results on the Success Rate and w.r.t. for V2V and V2I Communication

Fig. 10 (a) illustrates the rate of success of the V2I and V2V communication for our scheme. The success rate in the various quires groups is shown at Y-axis, each group represents queries of a certain value of *k* at X-axis. Black bars illustrate the true success rate delivered by our method, and the red bars illustrate a lower bound in the calculation of the quires should be used with regard to the above-mentioned method. There are three views from the Fig. 10 (a), primarily, our method delivers an average communication success rate. Secondly, the best average communication success rate is about 92 % of the abounded quires of 8 %, 50 % of them are not known, which means that in the worst case scenario, 5 % of all messages are diminished as a result of unknown messages. If we knew a method for constructing an optimal algorithm with logical and reasonable logic and tracking time, we could have a good boundary. Finally, quires with the greater k value are the more irregular.

The success rates for the value with $k = 2$ and 3 is about 40% greater than the success rates for the quires with the value of $k = 4$, and 5. Fig. 10 (b) demonstrates a relative (higher and better) anonymity level for our approach. The relative anonymities level y-axis is shown for different message groups; every group represents quires along a specific *k* value x-axis. Our approach represents relative anonymities level of 1:9 for quires with the value $k = 2$ which means that on average these quires are preserved with the value $k = 3.5$. Our method perform with small *k* values rather than greater values.

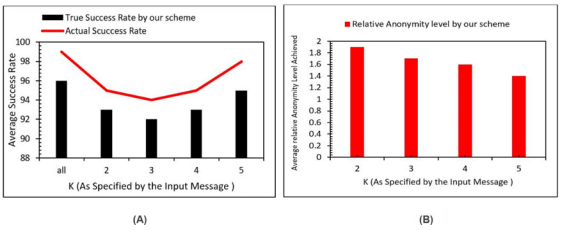

Figure 10. (a) Success rate for the different k values (b) Relative anonymity level for the diverse k value

The Fig. 11 illustrates how the network is occupied by the V2I and V2V communications over the time period. Very interesting results and prototype capabilities are implemented to cope with both simulation of vehicle communications and traffic. As predicted, the results of dissimilar arrangement designs indicate dissimilar behaviors of the framework in the dissimilar traffic environments. In the low flow of the traffic, the distribution of the queries through the V2V and V2I infrastructure is very weak, because of the network coverage. Only a short fraction of the networks, about 25%, can affect the distribution of the queries. In such events, it is quite possible that some vehicles may not receive the desired query. In the network where the traffic flow is medium, a large portion of the network was covered as illustrated in Fig: 11. The two thirds of the networks are secured in our case, in the better applicable terms, which means that the growing number of the vehicles will boost the network coverage`s and exceptional communications. In the third part, it is conceivable to achieve the full network coverage, which is absolutely predictable. In fact, in dense traffic conditions, the network links turn to work at their full extent, which means that the vehicle frequency is actually high and the progress of the vehicles tends to average on the vehicle unit. Under these circumstances, neighboring vehicles may be in the range of the wireless sensors and increase the network connectivity. However, in all the simulations, our method provide better results in large network coverage and when, it can be connected to a small network we need to control all the parts.

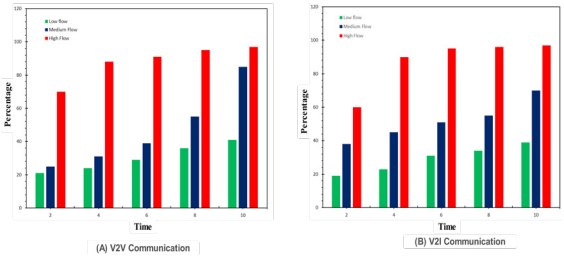

Figure 11. V2V and V2I communication w.r.t.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 61632009 and Grant 61472451, in part by the Guangdong Provincial Natural Science Foundation under Grant 2017A030308006, and in part by the High-Level Talents Program of Higher Education in Guangdong Province under Grant 2016ZJ01.

5. Conclusion

In this article we demonstrated an efficient method in which we preserve the query-based location and communication privacy in VANETs. There are two types of communications in VANETs V2V and V2I. In order to preserve communication privacy in both of them. We provide the trusted communication among the vehicles and infrastructure. Primarily, we used *Fs* along with Fog anonymizer CASPER, but this Fog anonymizer does not know the real location and queries of the vehicle driver due to the encrypted messages and *Fs* functionalities. In Fog computing, the algorithms of privacy preserving are run among fog nodes and cloud, because there is no problem of computation, processing, and storage for both sides, and these are sufficient. We create encrypted messages at initial level from the user side and send them to the *Fs*, and it also perform some encryption to secure the vehicle or vehicle driver because sometimes we cannot trust the Fog anonymizer or Fog anonymizer may be compromised, and the sensitive information will be reveal. Secondly we send all this information to Fog anonymizer and then Fog anonymizer anonymizes the query information and send it to the LBS. Then, it gets the desired results from the LBS and send them back to the vehicle`s or vehicle`s driver. The vehicle drivers transform the results and get the real query results.

REFERENCES

1. Alsarhan, A., Al-Dubai, A. Y., Min, G., Zomaya, A. Y. & Bsoul, M. (2018). A new spectrum management scheme for road safety in smart cities, *IEEE Transactions on Intelligent Transportation Systems*.

2. Shafiq, H., Rehman, R. A. & Kim, B.-S. (2018). Services and security threats in sdn based vanets: A survey, *Wireless Communications and Mobile Computing*.

3. Kouicem, D. E., Bouabdallah, A. & Lakhlef, H. (2018). Internet of things security: a top-down survey, *Computer Networks*.

4. Zhang, S., Wang, G., Liu, Q & Abawajy, J. H. (2017). A trajectory privacy preserving scheme based on query exchange in mobile social networks, *Soft Computing*, 1-13.

5. Chen, C., Liu, L., Qiu, T., Ren, Z., Hu, J. & Ti, F. (2018). Drivers intention identification and risk evaluation at intersections in the internet of vehicles, *IEEE Internet of Things Journal*.

6. Chen, S., Wang, G., Yan, G. & Xie, D. (2017). Multi-dimensional fuzzy trust evaluation for mobile social networks based on dynamic community structures, *Concurrency and Computation: Practice and Experience*, *29*(7).

7. Arshad, M., Ullah, Z., Ahmad, N., Khalid, M., Criuckshank, H. & Cao, Y. (2018). A survey of local/cooperative-based malicious information detection techniques in vanets, *EURASIP Journal on Wireless Communications and Networking*, *vol. 2018*(1), 62.

8. Boriboonsomsin, K., Durbin, T., Scora, G., Johnson, K., Sandez, D., Vu, A., Jiang, Y., Burnette, A., Yoon, S., Collins, J. et al. (2018). Real-world exhaust temperature profiles of on-road heavy-duty diesel vehicles equipped with selective catalytic reduction, *Science of The Total Environment*, *634*, 909-921.

9. Braun, A. & Rid, W. (2018). Assessing driving pattern factors for the specific energy use of electric vehicles: A factor analysis approach from case study data of the Mitsubishi i–miev mini car, *Transportation Research Part D: Transport and Environment*, *58*, 225-238.

10. Pournaghi, S. M., Zahednejad, B., Bayat, M. & Farjami, Y. (2018). Necppa: A novel and efficient conditional privacy-preserving authentication scheme for vanet, *Computer Networks*, *134*, 78-92.

11. Ydenberg, A., Heir, N. & Gill, B. (2018). Security, sdn, and vanet technology of driver-less cars. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 313-316). IEEE.

12. Wu, Q., Domingo-Ferrer, J. & Gonzalez-Nicol, U. (2010). Balanced trustworthiness,

safety, and privacy in vehicle-to-vehicle communications, *IEEE Transactions on Vehicular Technology*, *59*(2), 559-573.

13. Zhang, L., Wu, Q., Solanas, A. & Domingo-Ferrer, J. (2010). A scalable robust authentication protocol for secure vehicular communications, *IEEE Transactions on vehicular Technology*, *59*(4), 1606-1617.

14. Chim, T. W., Yiu, S.-M., Hui, L. C. & Li, V. O. (2011). Specs: Secure and privacy enhancing communications schemes for vanets, *Ad Hoc Networks*, *9*(2), 189-203.

15. Horng, S.-J., Tzeng, S.-F., Pan, Y., Fan, P., Wang, X., Li, T. & Khan, M. K. (2013). b-specs+: Batch verification for secure pseudonymous authentication in vanet, *IEEE Transactions on Information Forensics and Security*, *8*(11), 1860-1875.

16. Shim, K.-A. (2012). Cpas: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks, *IEEE Transactions on Vehicular Technology*, *61*(4), 1874-1883.

17. Jianhong, Z., Min, X. & Liying, L. (2014). On the security of a secure batch verification with group testing for vanet, *International Journal of Network Security*, *16*(5), 351-358.

18. Lee, C.-C. & Lai, Y.-M. (2013). Toward a secure batch verification with group testing for vanet, *Wireless networks*, *19*(6), 1441-1449.

19. Liu, J. K., Yuen, T. H., Au, M. H. & Susilo, W. (2014). Improvements on an authentication scheme for vehicular sensor networks*, Expert Systems with Applications*, *41*(5), 2559-2564.

20. He, D., Zeadally, S., Xu, B. & Huang, X. (2015). An efficient identity based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, *IEEE Transactions on Information Forensics and Security*, *10*(12), 2681-2691.

21. Zhong, H., Wen, J., Cui, J. & Zhang, S. (2016). Efficient conditional privacypreserving and authentication scheme for secure service provision in vanet, *Tsinghua Science and Technology*, *21*(6), 620-629.

22. Gregoriades, A & Sutcliffe, A. (2018). Simulation-based evaluation of an invehicle smart situation awareness enhancement system, *Ergonomics*, *no. just-accepted*, 1-28.

23. Zekri, A. & Jia, W. (2018). Heterogeneous vehicular communications: A comprehensive study, *Ad Hoc Networks*, *75*, 52-79.

24. Agbiboa, D. E. (2018). Conflict analysis in world class cities: Urban renewal, informal transport workers, and legal disputes in lagos, *Urban Forum*, *29*(1), 1-18. Springer.

25. Asuquo, P., Cruickshank, H., Morley, J., Ogah, C. P. A., Lei, A., Hathal, W., Bao, S. & Sun, Z. (2018). Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges and countermeasures, *IEEE Internet of Things Journal*.

26. Naserian, E., Wang, X., Dahal, K., Wang, Z. & Wang, Z. (2018). Personalized location prediction for group travellers from spatial–temporal trajectories, *Future Generation Computer Systems*, *83*, 278-292.

27. Fernandes, B., Rufino, J., Alam, M. & Ferreira, J. (2018). Implementation and analysis of ieee and etsi security standards for vehicular communications, *Mobile Networks and Applications*, 1-10.

28. Han, Y., Xue, N.-N., Wang, B.-Y., Zhang, Q., Liu, C.-L. & Zhang, W.-S. (2018). Improved dual-protected ring signature for security and privacy of vehicular communications in vehicular ad-hoc networks, *IEEE Access*, *6*, 20 209-20 220.

29. Hadiwardoyo, S. A., Patra, S., Calafate, C. T., Cano, J.-C. & Manzoni, P. (2018). An intelligent transportation system application for smartphones based on vehicle position advertising and route sharing in vehicular ad-hoc networks, *Journal of Computer Science and Technology*, *33*(2), 249-262.

30. Karim, A., Shah, S. A. A., Salleh, R. B., Arif, M., Noor, R. M. & Shamshirband, S. (2015).

Mobile botnet attacks-an emerging threat: Classification, review and open issues.

31. Yi, S., Li, C. & Li, Q. (2015). A survey of fog computing: concepts, applications and issues. In *Proceedings of the 2015 Workshop on Mobile Big Data* (pp. 37-42). ACM.

32. Truong, N. B., Lee, G. M. & Ghamri-Doudane, Y. (2015). Software defined networking-based vehicular adhoc network with fog computing. *In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (pp. 1202-1207). IEEE.

33. Mokbel, M. F., Chow, C.-Y. & Aref, W. G. (2006). The new casper: Query processing for location services without compromising privacy. In *Proceedings of the 32nd international conference on Very large data bases* (pp. 763–774). VLDB Endowment.

34. Năstase, L., Sandu, I. E. & Popescu, N. (2017). An Experimental Evaluation of Application Layer Protocols for the Internet of Things, *Studies in Informatics and Control*, *26*(4), 403-412. ISSN 1220-1766.

35. Velea, R., Ciobanu, C., Mărgărit, L. & Bica, I. (2017). Network Traffic Anomaly Detection Using Shallow Packet Inspection and Parallel K-means Data Clustering, *Studies in Informatics and Control*, *26*(4), 387-398. ISSN 1220-1766.