SDN-Based Secure VANETs Communication with Fog Computing

Muhammad Arif[1], Guojun Wang[1(✉)], Tian Wang[2], and Tao Peng[1]

[1] School of Computer Science and Technology, Guangzhou University,
Guangzhou 510006, Guangdong, China
arifmuhammad36@hotmail.com, csgjwang@gmail.com

[2] Department of Computer Science and Technology, Huaqiao University,
Xiamen 361021, Fujian, China
cs_tianwang@163.com

Abstract. We present a new VANETS architecture, which is a composition of two modules, software defined network (SDN), and Fog computing. The SDN-based framework gives the scalability, flexibility, programming capability, and the global information, while the Fog computing delivers delicate and locations-aware services that can meet the future demands of VANETs. The proposed framework can address the main problems of VANETs by providing vehicles communications (V2V), vehicle to infrastructures (V2I). We used hybrid SDN architecture and addition od security plane, proposed secure mechanism for communication. In addition, our proposed framework provides a textual awareness system that automatically and intelligently provides possible traffic safety and provides secure and fast communications. Results indicates that the proposed system provides the best results in terms of both type of communication in VANETs.

Keywords: VANETs · SDN · Vehicles · Fog computing
Cloud computing · Communication · Infrastructure

1 Introduction

VANETs have attracted a considerable attention in the modern era [10]. This potentially active and progressive area is designed to improve the road safety, increase traveling and traffic and efficacy, and give the comfort and convenience to the travelers and drivers [8]. V2I, and V2V communications are expected to increase in demand by increasing the growth of mobiles and onboard unite (OBUs) devices [6,11,30]. For providing the better services on the roads, VANETs can be very useful in provision of safety and the non safety programs [5,9]. For example, management and safety services for vehicles, social services, cloud services, and monitoring service. The VANETs is now a phenomena and supports a diversity of new protocols, and services [4,19], the traditional VANETs architecture for communication is illustrated in Fig. 1. Such as

G. Wang et al. (Eds.): SpaCCS 2018, LNCS 11342, pp. 46–59, 2018.
https://doi.org/10.1007/978-3-030-05345-1_4

traffic alert, route planning, background information and mobile cloud services, unbalanced traffic between multi-router topologies, and inappropriate network utilization [1,18,22,29].

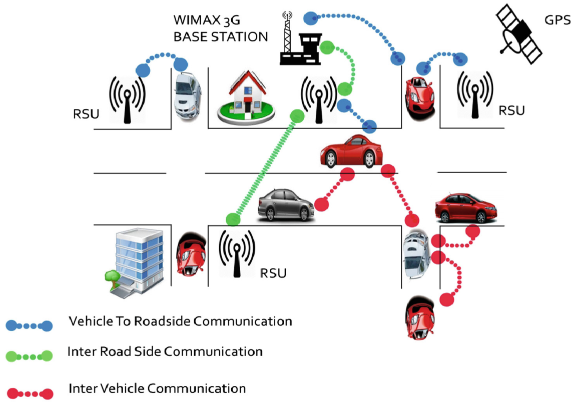
WIMAX 3G
BASE STATION
GPS
RSU
RSU
RSU
Vehicle To Roadside Communication
Inter Road Side Communication
Inter Vehicle Communication

Fig. 1. VANETs architecture and communication [4].

Some challenges are unresolved with the latest framework, such as increasing the connected devices, the use of effective resources and irregular traffic,privacy, security, geographical address, delays due to excessive traffic and unreliable connections, and QoS [7,15]. Even if, self-organized, distributed networks mode, such as MANETs, can be used to resolve the problems [26,28]. In these cases, the absence of a enthusiastic methods for connections and resource management makes the some services inaccessible. Therefore, open and flexible architecture of vehicles is a key requirement that allows testers to conduct their testing in production of environment, and improve the network resource management, applications, and the users [7,16]. To handle the above mentioned challenges, we look at the Software Defined Networks (SDN) and Fog computing. Today, SDN has emerged as a commonly used SDN protocol as a flexible method for controlling the networks in a free flow and in efficient way [18]. SDN Flexibility is an interesting method that can be used to meet the concerns of the VANETs. For employing the SDN policies and rules to VANETs, there is plenty of planning and flexibility available in today's wireless distribution network [14]. For enabling the V2I and V2V applications and services and facilitate the network management [20].

In this article, we focus on using SDN and Fog Commuting (FC) for secure communication. In particular, we have attention on the framework, services, operations and communication of the software-defined VANETs with FC.

The reminder of the paper is organized as follows. Section 2, is about the overview of the system design and architecture. Section 3, is about results, discussion, and performance analysis, and the last section is about the conclusion.

2 Overview of the System and Design

The flow of the proposed framework is illustrated in the Fig. 2, for the secure communication among the vehicles and the cloud and transportation servers, we used SDN controller (SDNC) and FC. We used hybrid SDNC with security plane as shown in Fig. 3 for scalability, flexibility, security, programmability, and for the global information. While, the FC provide location-awareness and delay-sensitive services, for satisfying the demand of the future VANETs. The main components we used in our system are given below,

- SDNC is a logical essential intelligence entity of our framework. The SDNC controls the actions of the whole network.
- SDN wireless node: this node is controlled by SDNC, also receive the instructions from SDNC to execute the processes.
- SDN RSUs: the SDN RSU also controls by the SDNC, and they are fixed alongside the roads, and used for forwarding the data, All RSUs works as fog devices.
- SDN Roadside Controllers (RSUC): A group of the RSUs connect to the RSUC priors to approaching the SDNC to bandwidth connections. RSUC Open Flow is enable and control by SDNC. In addition to data transmission responsibility, RSUC also stores road information and provides emergency and necessary services. All RSUC works as fog devices under the orchestration of SDN controller.
- Fog Computing: Fs acts as an intermediate tier between SDNC and the cloud server to provide the secure transmission of communication in VANETs.

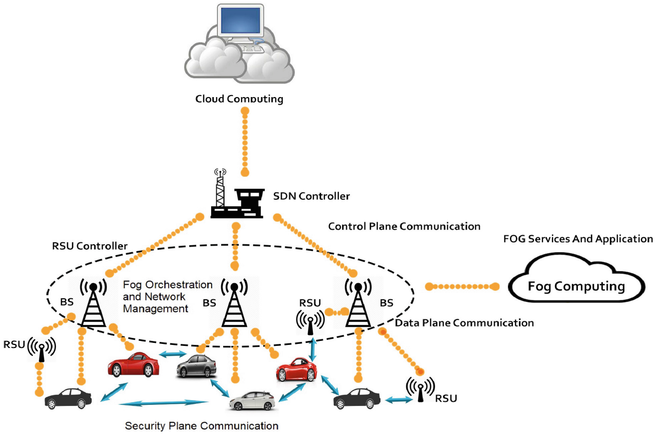
Cloud Computing
SDN Controller
Control Plane Communication
FOG Services And Application
RSU Controller
Fog Orchestration and Network Management
BS
BS
RSU
BS
Fog Computing
Data Plane Communication
RSU
RSU
Security Plane Communication

Fig. 2. VANETs architecture based on SDN controller and fog computing.

2.1 Software Defined Networks

The main idea behind SDN is the collision between the control and the data planes [13]. In the SDN, the network devices like switches and the routers are based on the policies and rules. These rules are created or changed before being sent to network devices. The overall behaviours of the network is only determined by the control logic [21]. This new network paradigm has many advantages correlated with the traditional distribution methods. First, the network is being developed and deployed in applications, functions and protocols. In the SDNC, it is very simple to program, modify, manipulates and configures a centralized protocols, without the need for independent access and configuration of network hardware across the networks [21].

Second, SDN-based architectures are network-based controllers that have global knowledge of network status that can control the network infrastructure independently of the vendor. These network devices simply accept control policies without understanding and enforcing the standards of different network protocols and directly controls, programs, synchronize, and managed the network resources in SDNC. For SDNC, the communication protocol is the main requirement for control and the data planes.

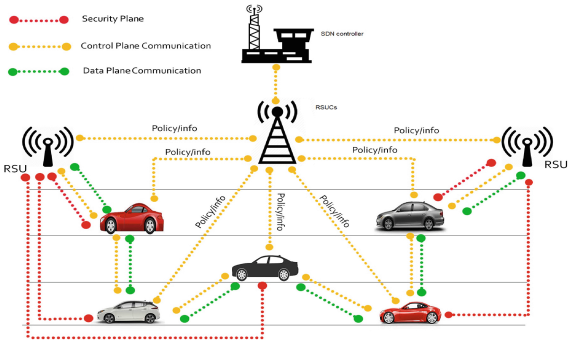

Fig. 3. Software defined VANETs architecture and communication.

2.2 Fog Computing (FC)

Recently, FC has become an active cloud-related research area. It was incorporated by the Cisco in 2012 [23, 27]. It is extended paradigm of the cloud computing where network edge is employed for data processing and services on contrary to the existing technique in which it 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 it closer to end-users. FC also incorporates core cloud services. It also changes conventional data centres into heterogeneous and distributed platforms [24,25]. Therefore, the FC support the applications of IOT in vehicular network, actors/sensor networks and the industrial automations that require the processing of contexts awareness and sensitive delays [12,17].

Privacy in Fog Computing. The most concerning problem of user is the risk of privacy leakage in VANETs. In fog computing, the algorithms of privacy preserving are run among FC nodes and cloud, because there is no problem of computation, processing, and storage for the both sides, and these are sufficient. And the running algorithms are resources barricade at end devices level, they usually collect the data for the end devices 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.

2.3 Basic Operations

The communication of SDNC in proposed framework are composed on three parts, the security, control, and the data planes. We used hybrid control mode of SDN with little modification of security plane in it, to provide the better security for vehicles communication as shown in Fig. 3. Data control communications are for flow of rules and policies regulations, while, data plan communication is for data transfer. The security control plane send the security keys to the RSUs, where the RSUCs collect all the keys, combined them and send to the SDNC as illustrated in Fig. 3. By using of the FC, we select the mode with the hybrid control, because in this mode the controller does not have complete controls over the network, but it propagate the policies and rules with the RSUCs through RSUs. For example, in preference of providing specific flow rules and policies, SDN provides an abstract policy called policy information, where the particular behaviours are determined by the RSUs and RSUCs, its depends on their local information. RSUC data is then sent to the Fog server via SDNC for the global and continuous goals. To manage the network topology, the link layer structure in any vehicle can be used for tracking accessible messages continuously to learn neighbouring knowledge. This knowledge, contains the vehicle traffic information, route map, speed, position, and the sensor information.

SDNC not only receives the vehicles information from the RSUs and RSUCs, but, also transmits information from the RSUs and RSUCs to the vehicles. So, it can create a global connected graph of the SDN, RSUCs and RSUs, and other information essentials for the different services. The RSUCs also receive traffic knowledge from an RSUs, so they can process some supervisory information without full knowledge of the SDNC. RSUs and RSUCs provide local and appropriated information with short-term awareness and location features. These RSUCs and RSUs merge the sub quires and security keys and then send to the SDNC.

In the FC, both the edge devices and the data centers, support indirect sources and services. The RSUs and RSUCs, send the information through SDNC to the Fog server, also share resources for vehicle control. To enabled the FC architecture in the software defined VANETs, SDNC, RSUCs and RSUs provide not only the SDN capabilities but also Virtualization to enable Fog and cloud services [2,3]. Hence, a hyper visor, which is a small-level middle-ware, must be run on these physical devices to support virtual machine abstraction (VM). Services are hosted on these VMs that allow the transmission and re-service of the service.

2.4 V2V and V2I Communication Mechanism with Security Plane

In this section we only provide the secure communication mechanism for V2V and V2I communication in the VANETs, by using SDN and Fog computing.

For the secure communication plan we used three types of data plan in our proposed system, namely, security plan, control plan and data plan. Where the security plane is used to forward the encrypted keys. An active switch also acts as a secures channel for communication to the SDNC, which allows data packets and remote streaming packets are sent through the SDNC by using free stream protocols [13]. SDNC have the responsibility for deciding whether to add, remove, and modify the policies, rules, and actions in the flow of traffic through free flow, thus enabling scheduling to automatically configures the VANETs networks. SDN services and applications communicate directly to their needs and network activities through the North-bound (NBI) user interface APIs to the SDNC.

The software component required to construct a SDN architecture to ensure the cooperation of integration. The SDN function and the fog calculation enter the vehicular network. The RSUs and the BS can match the Mayor Orchestration is based on MANO architecture. In this way, BS and RSUs need a management mechanisms to allow data transfer the information and rules to the managed services. Fog node must acknowledge the dissimilar decisions, for example, quality of service (QoS), quality of experience (QoE), network technology,topology, operators, to determine its location and time.

Request Generation Process. The anonymous inquiry process is generated by the vehicle V, which intend to approach the service giving by the transportation server or cloud server. There is no communication overhead for the V in execution of inquired queries for communication process, V commitments to firstly define M as message and the k as privacy preferences. Then, V added the M identity mid and transmit the M into the k data movement generating the set of messages $\{m1, m2, \ldots, mk\}$ and set of keys $K = \{k_1, k_2, \ldots, k_m\}$. The encrypted messages are distributed among the vehicles communication range in the VANETs, and the derived keys are sent to the RSUs through security plane, where the RSUCs collect all the keys and send to the SDNC. Distinctive methods (it depends on the position of the vehicles or the state of the network) can be implemented for the broadcasting of messages in the vehicles. Here in our method, we use a easy approach for the sharing of messages among the vehicles in VANETs. Our broadcasting method for communication among the vehicles performs as follows. The initiator V encrypts all the encrypted messages mi using the set of keys Ks shared among vehicles and RSUs, Fs and the affix mid, that $\{mi = \{EKs(mi)||mid\}\}$ for every $\{i = 1, k\}$. Due to the, existence of the id of the message mid in all the messages, allow the vehicles to recognize the dissimilar sub-messages associated to the same M. Query initiator V randomly chose $k-1$ vehicles Vs in his communications ranges, then send the messages from $\{m1 \Rightarrow mk\}$to each of them. It then send these messages to SDNC via Fs, RSUs and RSUCs, where these RSUs and RSUCs works as fog devices. Upon accepting the messages mi from the every vehicle in the communication range, then $V1$ first checks the mid. If the vehicle is already acknowledged to send the message with same mid, $\{mid \in Sent\}$, $V1$ transmit mi to next vehicle $V2$ in the communications range. After the transmission process every selected vehicle V separately sends the encrypted messages received by the SDNC. These encrypted messages from all the vehicles are forwarded to SDNC through RSUCs and the FS. Now SDNC can decrypt the each message incrementally, reconstruct the messages and sends it to the cloud server.

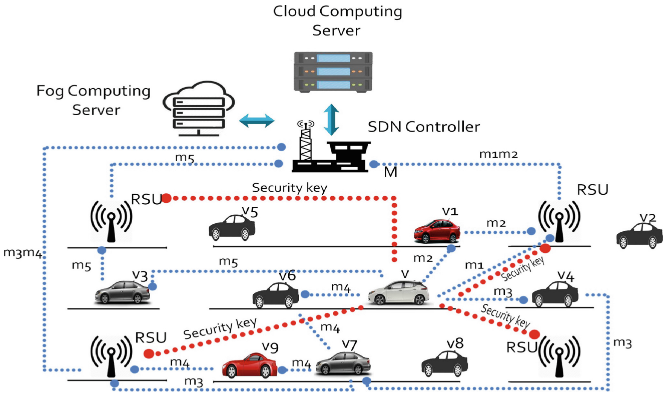

Fig. 4. Anonymous request based on SDN and fog computing.

Figure 4 shows an example of communication among the vehicles. Where, the vehicle V generate and forward a encrypted message to the next neighbouring vehicles, while the selected vehicles in the communication range sends the encrypted messages to the SDNC through RSUs and RSUCs. In the given example, the inquired V describe $k = 5$ then distribute M into the five sub-messages $\{m1, \ldots, m5\}$. Messages are then encrypted with the ABE method, generated the set of keys $K = \{k_1, k_2, \ldots, k_m\}$ and shared between V and SDNC, and mid is appended with each of the sub messages. The set of keys are directly forwarded by the particular V to the all nearest RSUs, from there the RSUCs collect all keys and send to the SDNC through FS. The inquired vehicle V sends the encrypted message $m1$ to SDNC and transmits the remaining $k-1$ messages to other vehicles in communications ranges. Categorically, the sub-message $m2$ and the $m5$ are forwarded to the vehicles $V1$ and $V3$ that forward these messages to the Fs. Considering $v4$ not accept for transmit sub-message $m3$, sub-message $m3$ then gets a route $V4 \Longrightarrow V7$. The sub-message $m4$ gets a route $V6 \Longrightarrow V7 \Longrightarrow V9$ because, when the sub-message is acknowledged by $V7$ and $V7$ considers that it has already get sub-message $(m3)$ with same $mids$, then it forward sub-message $m4 \Rightarrow V9$. Lastly, vehicles $V, V1, V3, V7$, and $V9$ sends the sub-message to SDNC via FS, RSUs and RSUCs.

Response Generation Process. The response generation process is anonymous, because of encryption and decryption, and no one can track the original vehicle by tracking the communication process. If in the case, the cloud or transportation server, compromised no one can track the communication, because they did not know the exact query or information of the vehicles.

Figure 5 represent an illustration of anonymous feedback to the query in Fig. 5. Encrypted Queries Mr are broadcast to all the vehicles utilized in Fig. 5, that are, $\{V, V1, V3, V7, V9\}$. When V collects the message, he can decrypt it with keys Ks shared by the SDNC. The auxiliary vehicles deleted this message Mr, because they do not have the key.

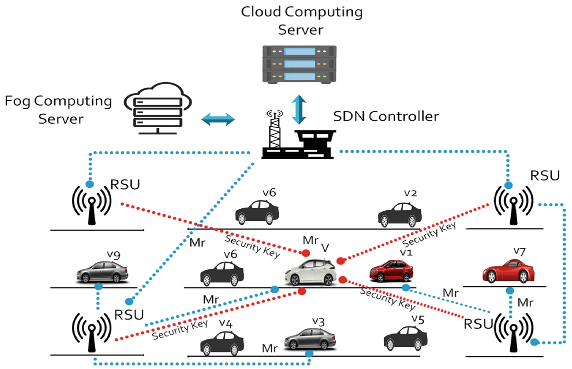

Fig. 5. Anonymous response based on SDN and fog computing.

3 Experiments, Results and Discussion

3.1 Experimental Setup and Simulation

For the simulation, we used Veins model for simulation along with SUMO and OMNet++ environment. The parameters we used in simulations are presented below in the Table 1.

Table 1. Description of the parameters

Parameter	Value
Simulation framework	OMNet++, Sumo and Veins
Area	50–100 km^2
Vehicles	100–200
No of RSU	25–50
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	−80.0dBm
Antenna height	1–1.5 m
Type of the antenna	Omnidirectional
Network layer	802.11p and IEEE 1609.4
ROI size	9 km^2
Transmission range	500 m

3.2 Security Analysis

Our secure communication method provides complete privacy protection because it guarantees the privacy of the vehicle and the anonymity of the link in terms of both the vehicle and the server. Our approach preserves the communication privacy of vehicles and protects against privacy breaches by using secure communication methods as well as SDNC and FC. In order to check the privacy of the vehicle, through our proposed method, when establishing a new communication session with the cloud or transport server, the vehicle always generates a set of keys for its own message. Therefore, it is computationally impossible for a vehicle or group of vehicles to notice the true identification of other vehicles and to link different communication sessions or authentication *mids* to the same vehicle.

For both types of communication (V2V and V2I), the cloud and transport server does not know the real information about the communication due to encrypted communication. The desired result produced by the cloud or transport server is the user result of all vehicles within the communication range, not the enemy, nor the cloud server, knowing that the result is returned to the active user. Therefore, they cannot access location information related to the vehicle. The fog server was unable to know the original query information for each vehicle because we had performed encryption through the vehicle driver and SDNC.

The communication and location information from every vehicle to the Fog server is encrypted queries and information. The decryption function parameters are only known by the vehicles Vs and SDNC. The trusted entity could not find the original query information about the communication. Even if the SDNC or fog server is attacked by an enemy, the information of the vehicle will not be revealed due to the fog server privacy.

The vehicles does not know the queries of the other vehicle while communicating with each other. The FS accurately obtains the expected results for every vehicle, and everyx vehicle can easily obtain their own results without knowing the identity of other vehicles. Even if some malicious cars cooperate, they can't understand other problems with trusted vehicles.

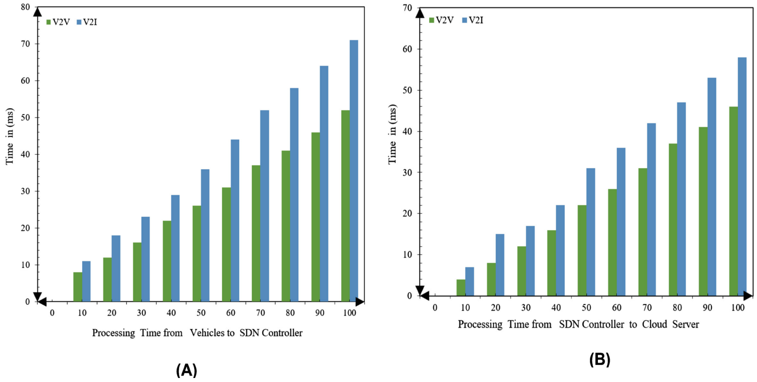

Fig. 6. (A) Processing time from vehicle to SDNC, (B) Processing time from SDNC to cloud server

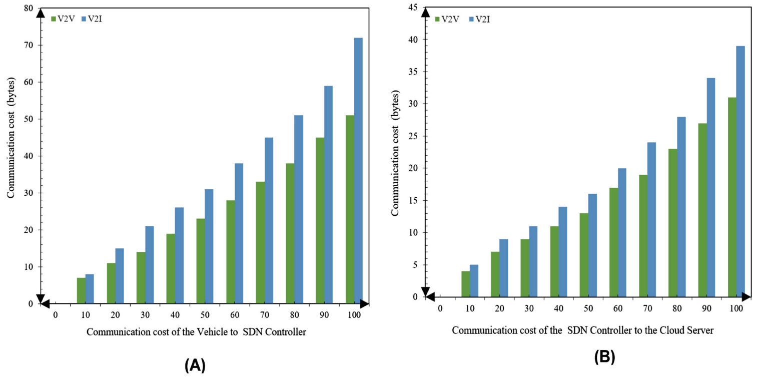

Fig. 7. (A) Communication cost from vehicles to SDNC, (B) Communication cost from SDNC to cloud server.

3.3 Performance Analysis

There are four entities in our proposed scheme, and we calculate the cost of computation of these four entities, the complexity of vehicle is the $O(N + mk)$, where N, and m, and ks are the numbers of the vehicles, messages, and security plan respectively. The ruining time of SDNC is the $O(N + m + K)$, where the N shows the vehicles and m are the messages, and K is the set of security keys, because the SDNC is only responsible to collect the messages from the vehicle encrypt them and forward to the Fog server. The running time of the fog server is the $O(N + logm)$, where N are the vehicles and m are the messages. The complexity of cloud server is $O(N + logm + mr)$, where the N are vehicles and m are messages and r are the required results. The total complexity of proposed system is given below.

$O(N + m + K + N + logm + N + logm + mr)$.
$O(3N + 2m + k + 2logm + mr)$.
we excluded the constant, so the final computational cost is given below.
$O(N + m + k + logm + mr)$.

The communication cost among the vehicles and the SDNC becomes $O(Ck+D)$, where C and D are the constants, and we reduce it as $O(k)$. The communication cost between the SDNC and the Fog server is $O(Ak + B)$. Lastly, we examine the communication cost between the SDNC and the cloud server. So, the communication cost is $O(KC * mD)$, where C and D are the constants. So the total cost among the vehicles and the cloud server is $O(k + AK * mB)$.

Mainly the complexity of the framework depends on its algorithms. To evaluate and analyse the complexity, we perform some simulations, in simulations we calculated the communication cost and time complexity.

Figure 6(a, b), shows the time of processing for vehicles in our proposed method. The x-axis and Y-axis contain the vehicles and time information respectively.

The Fig. 6(a, b) contain the processing time of the vehicles with SDNC and cloud computing. to achieve this goal, we simulate approximately 100 vehicles, and it is clearly shown that, if the all vehicles are in the communication range, then the processing time is very low. Figure 6(a, b) shows the time of processing from the Vehicles to the SDNC and from the SDNC to the cloud server, from the Figs, we can clearly analyse that the time of processing for this environment is also very low.

The communication cost (CC) of the proposed system is shown in the Figs. 7(a, b). The information about vehicles and memory (bytes) is listed on x-axis and Y-axis respective. the CC is represented in Fig. 7(a), when vehicles start the communication through RSUs or by others vehicles that are available in the communication range. Figure 7(b) represents the CC from SDNC to the cloud server.

The results from the Figs shows that our proposed scheme have very low CC, when all vehicles are in the communication range. From the Fig. 8, the execution time required by the OBU to generate the messages for the communication between V2V and V2I is very low. It is seems that in very short time span the maximum numbers of the messages are communicated between the vehicles.

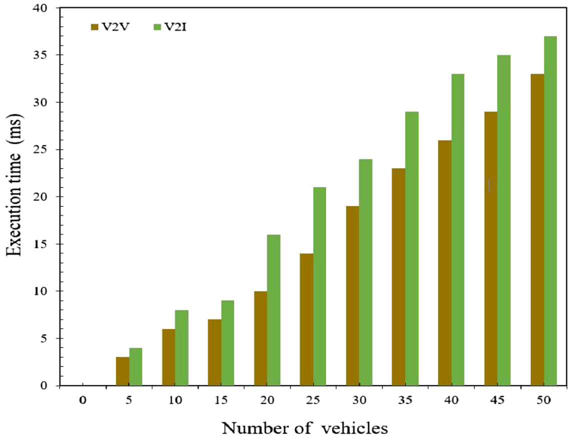

Fig. 8. Execution time of messages

4 Conclusion

In our proposed approach, we preserve the communication privacy in VANETs. There are two types of communications in VANETs V2V and V2I. In order to preserve communication privacy for V2V and V2I, we provide the trusted communication among the vehicles and infrastructure. In V2V and V2I communication privacy, primarily, we used SDNC along with Fog computing. In SDNC, we used security, data, and control planes, for sending the keys and data to the RSUs generated by the vehicle. Fs operated as and intermediate tier between SDNC and cloud server to provide the secure transmission of communication in VANETs. We create encrypted messages at initial level from the user side and send to the SDNC, where the SDNC combined the keys as well as the messages, decrypt the message. After this, we send all these information to the cloud server for the desired results, after getting the results the SDNC transmit all the results to the vehicles through FS and RSUC, RSU, where the vehicle driver received the results with keys and decrypt the results.

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.

References

1. Arif, M., Alam, K.A., Hussain, M.: Application of data mining using artificial neural network: survey. Int. J. Database Theory Appl. **8**(1), 245–270 (2015)
2. Arif, M., Mahmood, T.: Cloud computing and its environmental effects. Int. J. Grid Distrib. Comput. **8**(1), 279–286 (2015)
3. Arif, M., Shakeel, H.: Virtualization security: analysis and open challenges. Int. J. Hybrid Inf. Technol. **8**(2), 237–246 (2015)
4. Arif, M., Wang, G., Balas, V.E.: Secure VANETs: trusted communication scheme between vehicles and infrastructure based on fog computing. Stud. Inform. Control **27**(2), 235–246 (2018)
5. Arif, M., Wang, G., Chen, S.: Deep learning with non-parametric regression model for traffic flow prediction. In: Proceedings of IEEE 16th International Conference on Dependable, Autonomic and Secure Computer, 16th International Conference on Pervasive Intelligence and Computer, 4th International Conference on Big Data Intelligence and Computer, and 3rd Cyber Science and Technology Congress, pp. 681–688. IEEE, August 2018
6. Arif, M., Wang, G., Peng, T.: Track me if you can? query based dual location privacy in VANETs for V2V and V2I. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1091–1096. IEEE (2018)
7. Ghosal, A., Halder, S.: Building intelligent systems for smart cities: issues, challenges and approaches. In: Mahmood, Z. (ed.) Smart Cities. CCN, pp. 107–125. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76669-0_5
8. Guerrero-Ibáñez, J., Zeadally, S., Contreras-Castillo, J.: Sensor technologies for intelligent transportation systems. Sensors **18**(4), 1212 (2018)
9. Klingler, F., Cohen, R., Sommer, C., Dressler, F.: Bloom hopping: bloom filter based 2-hop neighbor management in VANETs. IEEE Trans. Mob. Comput., 1 (2018)
10. Li, H., Lu, R., Misic, J., Mahmoud, M.: Security and privacy of connected vehicular cloud computing. IEEE Netw. **32**(3), 4–6 (2018)
11. Ligo, A.K., Peha, J.M.: Cost-effectiveness of sharing roadside infrastructure for internet of vehicles. IEEE Trans. Intell. Transp. Syst. **19**, 2362–2372 (2018)
12. Liu, Q., Wang, G., Liu, X., Peng, T., Wu, J.: Achieving reliable and secure services in cloud computing environments. Comput. Electr. Eng. **59**, 153–164 (2017)
13. Naman, A.T., Wang, Y., Gharakheili, H.H., Sivaraman, V., Taubman, D.: Responsive high throughput congestion control for interactive applications over sdn-enabled networks. Comput. Netw. **134**, 152–166 (2018)
14. Nobre, J., et al.: Vehicular software-defined networking and fog computing: integration and design principles. Ad Hoc Netw. **82**, 172–181 (2018)
15. Peng, S., Wang, G., Zhou, Y., Wan, C., Wang, C., Yu, S.: An immunization framework for social networks through big data based influence modeling. IEEE Trans. Dependable Secure Comput. (2017)
16. Peng, T., Liu, Q., Meng, D., Wang, G.: Collaborative trajectory privacy preserving scheme in location-based services. Inf. Sci. **387**, 165–179 (2017)
17. Rahmani, A.M., et al.: Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. Future Gener. Comput. Syst. **78**, 641–658 (2018)

18. Rego, A., Garcia, L., Sendra, S., Lloret, J.: Software defined networks for traffic management in emergency situations. In: 2018 Fifth International Conference on Software Defined Systems (SDS), pp. 45–51. IEEE (2018)
19. Singh, G.D., Tomar, R., Sastry, H.G., Prateek, M.: A review on VANET routing protocols and wireless standards. In: Satapathy, S.C., Bhateja, V., Das, S. (eds.) Smart Computing and Informatics. SIST, vol. 78, pp. 329–340. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-5547-8_34
20. Teniou, A., Bensaber, B.A.: Efficient and dynamic elliptic curve qu-vanstone implicit certificates distribution scheme for vehicular cloud networks. Secur. Priv. **1**(1), e11 (2018)
21. Truong, N.B., Lee, G.M., Ghamri-Doudane, Y.: 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 (2015)
22. Wang, F., Jiang, W., Li, X., Wang, G.: Maximizing positive influence spread in online social networks via fluid dynamics. Future Gener. Comput. Syst. **86**, 1491–1502 (2018)
23. Wang, T., et al.: Data collection from WSNs to the cloud based on mobile fog elements. Future Gener. Comput. Syst. (2017, in press). https://doi.org/10.1016/j.future.2017.07.031
24. Wang, T., Zhang, G., Bhuiyan, M.Z.A., Liu, A., Jia, W., Xie, M.: A novel trust mechanism based on fog computing in sensor-cloud system. Future Gener. Comput. Syst. (2018, in press). https://doi.org/10.1016/j.future.2018.05.049
25. Wang, T., et al.: Fog-based storage technology to fight with cyber threat. Future Gener. Comput. Syst. **83**, 208–218 (2018)
26. Xing, X., Wang, G., Li, J.: Collaborative target tracking in wireless sensor networks. Adhoc Sens. Wirel. Netw. **23**, 117–135 (2014)
27. Yi, S., Li, C., Li, Q.: A survey of fog computing: concepts, applications and issues. In: Proceedings of the 2015 Workshop on Mobile Big Data, pp. 37–42. ACM (2015)
28. Zhang, Q., Liu, Q., Wang, G.: PRMS: a personalized mobile search over encrypted outsourced data. IEEE Access **6**, 31541–31552 (2018)
29. Zhang, S., Wang, G., Bhuiyan, M.Z.A., Liu, Q.: A dual privacy preserving scheme in continuous location-based services. IEEE Internet of Things J. **5**, 4191–4200 (2018)
30. Zhou, Z., Dong, M., Ota, K., Wang, G., Yang, L.T.: Energy-efficient resource allocation for D2D communications underlaying cloud-RAN-based LTE-A networks. IEEE Internet of Things J. **3**(3), 428–438 (2016)