ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2021.0362

RSA BASED SECRET KEY GENERATION AND AUTHORIZATION METHOD IN CLOUD BASED VANETS

B. Chithra[1] and B.M. Rajesh[2]
[1]*Department of Computer Technology, SNMV College of Arts and Science, India*
[2]*Department of Information Technology, Dr.NGP Arts and Science College, India*

Abstract

Private transportation has become a daily need for most people nowadays. Because of the increased use of private transportation by modern society, road accidents have become a major issue. Vehicular communication is one of the methods to reduce the number of dangerous accidents. It is possible to communicate between two vehicles, Known as Vehicle to Vehicle Communication (V2V). Road Side Unit (RSU) is a communication with a specific fixed unit. If communication is established between the vehicle and nearby infrastructure (V2I), accidents can be avoided. Inter Vehicular communication is the term for this type of communication. It also lets vehicles share information such as post-accident investigation, safety information for accident prevention, traffic jams, and many more. Europe and North America are at the forefronts of research to conclude vehicular communication standards. It recognizes technical specification for enabling the communication between vehicles and the road infrastructure and between the various manufacturers. In the existing method, Cloud-based VANET helps to monitor the road condition. Through the connected Vehicular Ad-hoc Network (VANET) and cloud computing technologies, the entities in VANET were able to access the valuable storage and computing services made available by some cloud service provider. The benefits cannot be given away for free because their combination introduces various privacy and security requirements for VANET applications. The authority should monitor real-time road condition using a cloud server, so sound responses to emergencies can be made on time, according to the cloud-based Road Condition Monitoring (RCoM) scenario examined here. Vehicles on site should report information if any dangerous road condition is detected, such as geologic hazards or accidents. Three major issues are discussed in RCoM. An efficient RCoM method was suggested to address these three issues to analyze its efficiency theoretically and to demonstrate its practicality through experiments. They were generated using random numbers and help us in authorization process. So, the malicious vehicles easily identity it. To resolve the issues mentioned above, one Improved Road Condition monitoring system (IRCOM) was initiated. Using the random key generator, the first sub authority delegation is performed, and by using the RSA algorithm, the vehicle registration is attained by generating individual keys. The distribution of the token is based on the individual key and time stamp assigned to each vehicle. Cloud will categorize the received report using the key, token and time stamp. Finally, the route authority will decode the reports and, if necessary, will take the appropriate action.

Keywords:

Vehicle to Vehicle Communication, Road Side Unit, Vehicular Ad-hoc Networks, Connected Vehicular Cloud Computing, Dedicated Short Range Communication

1. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs) technology has become important research in recent years. VANET is a form of network that develops from creating a network of cars to meet particular needs or situations. Vehicles use this network for communication in urban environments and highways. In VANET, there is a lot of disagreement on vehicle and individual security [1], QoS provisioning, and high connectivity & bandwidth. VANETs major objective is to assist a collection of vehicles, without any central base station or controller, to establish and maintain the communication network. Vehicular communication is one of the ways to reduce hazardous accidents. A vehicular ad-hoc network is used to communicate between the moving vehicles. Vehicle-to-Infrastructure (V2I) is known as communication between two vehicles (V2V) or communication between infrastructures such as an RSU. The main aim of VANET is to establish a secure, efficient and reliable protocol [3] [4].

Connected Vehicular Cloud Computing (CVCC) has been introduced in recent years, integrating VANET with cloud computing technology. With CVCC, all entities can benefit from cloud computing, i.e., storage service and computing provided by some cloud service provider. The vehicle communicates with some Road Unit to attain a token. Using this token, the vehicle generates a report, and the same is uploaded to the cloud server for processing [5];[6]. Many efforts were made to address safety issues in VANETs, such as to ensure authentication, non-repudiation, integrity and message privacy.

The authority monitors the real-time road condition with the help of a cloud server in the RCoM method to respond to emergency cases timely. When a terrible road condition is observed, such as a geologic hazard or an accident, vehicles on the site can submit this information to the authority's cloud server. First, the vehicle should be authorized before uploading it to the cloud server. Secondly, to ensure privacy, the data should be reported in the ciphertext format so that the cloud server can differentiate reported data from various vehicles without compromising confidentiality. The final step is to check whether the legitimate vehicles report the road conditions to check the report source by the authority and the cloud server [7]. An improved Road Condition Monitoring System (IRCOM) was introduced in this paper to overcome the issues mentioned above. The random key generation is used to perform the first sub authority delegation by using the RSA algorithm. The vehicle registration is attained by generating individual keys.

2. LITERATURE REVIEW

Al-Otaibi et al. [8] developed a new privacy-preserving vehicular rogue node detection approach utilizing fog calculation. The safety of the vehicle, computation efficiency and communication between the vehicles are improved by avoiding the interchange of traffic information in between the vehicles, and the communication is allowed only via Road Side Units (RSUs). One RSU authentication technique including one technique that permits RSUs for identifying and stopping the vehicles from

giving fake traffic information so as to improve the efficiency and accuracy of VANETs. Therefore, the experimental results show that this approach detects rogue vehicles precisely, protects the system from colliding with other vehicles, reduces overhead and provides enhancements in the data processing.

Agarwal et al. [9] suggested a new approach for providing Time of Arrival (ToA) based localization, collision avoidance and speed-based lane variation in Vehicular Ad Hoc Networks (VANETs). The ToA based algorithm is designed for locations in which the strong GPS signals are unreachable. Some of the applications of collision avoidance are explained by utilizing camera-based surveillance and automatic braking. The feasibility of this approach is defined by network simulator-2 (NS-2) and Simulation of Urban Mobility (SUMO). In order to attain efficient and smart remote traffic monitoring, one mobile application interface is developed for the on=board-unit.

Tan et al. [10] designed an Emphasizing secure authentication and road message dissemination in VANETs. The certificate less cryptographic scheme is employed for authentication and key distribution processes. And a proper road message dissemination scheme is designed. Later, the security analysis and performance evaluation are performed accordingly. This method can able to bring road information services inaccurate time so as to improve driving experience and safety of the user.

Zhang et al. [11] designed an identity-based method for signature hierarchical aggregation and responding to anonymous vehicle-generated messages rapidly. In this, the identity-based vehicles and RSUs are used so that the overheads of certification verification and management are made easier. An aggregate signature is generated in accordance with synchronized common strings within a short period of time. By this approach, the waiting time of vehicle before the start of the batch verification process is reduced, and also the storage/transmission overhead of an entity is minimized.

Sheikh and Liang et al. [12] discussed the architecture, challenges and security issues of recent methods of VANETs. For assuring secure communication in VANETS, the security techniques are evaluated elaborately. The mobility and network simulation tools and the performance of the authentication techniques that are utilized for protecting the vehicular network from false messages and malicious nodes are discussed. At last, the safety and comfort applications of VANETs are described. Also, the applications of VANETs, including the recent trends of VANETs, are discussed.

Zhang et al. [13] described the generation of vehicular sensor networks (VSNs) and their applications and characteristics. Also, the traditional data transmission techniques and traffic abnormal data identification in VSNs are discussed. At the same time, the present abnormal data detection method is also discussed. The traditional data transmission techniques are divided into multi-hop routing-based transmission and one-hop dedicated short Range Communication (DSRC) based transmission. Particularly, the multi-hop routing-based transmission was detailed via routing information and data transmission techniques.

Radopoulou et al. [14] performed an evaluation of the present condition of road asset observation. The present condition of this observation process is divided into type of gathered data, type of asset covered and amount of data provided. This mentioned classification is analyzed with respect to efficiency, accuracy, overall improvement to the present method and cost. The results of this method depict that this approach has low efficiency and also fails to provide a better solution to the issue of road asset condition observation process.

Forslöf and Jones et al. [15] designed an approach that evaluates the condition of the road by minimizing the operating/maintenance costs of road and vehicle and improving ride comfort and safety. The road roughness data is gathered by utilizing a built-in vibration sensor in smartphones. As the data is gathered often, the user can be able to observe the changes in roughness over a certain period of time. The continuous data gathering process provides early warning about the damage so that it is easy to find new approach to use in the road maintenance work. The gathered data are transmitted to other geographical information systems ((GIS) or road management systems.

Sattar et al. [16] suggested a road surface monitoring method for assuring smooth and safe road infrastructures to users. The anomalies in roads such as bumps, potholes and cracks are identified by this approach. Smart-phone based sensing techniques are widely used nowadays, with a large number of sensors integrated with smartphones in recent times. But the sensors embedded in smartphones operate at low frequency, and so the accuracy of anomalies identification is reduced. In this, the use of smartphones in anomaly detection of the road surface is discussed.

Zhang et al. [17] designed a privacy-protecting and secure communication approach for establishing vehicle cloud (VC) and data dissemination process. This approach operates based on the identity of a public key cryptosystem and permits a group of vehicles to anonymously and securely creates a VC. Here joining and leaving algorithms are designed so as to enable cloud user dynamics. After the formation of VC, the user can send messages to VC anonymously and securely.

Liu et al. [18] suggested a model for protecting the privacy and security of group communication. This approach provides highly balanced communication performance and speeds up the encryption and decryption processes by transforming dynamic session secret key having high computational capacity than the On-Board Unit (OBU) via fixed roadside unit (RSU). For enhancing authentication efficiency, and executing anonymous authentication mechanism effectively, the batch authentication strategy and shared key mechanism are employed in RSUs and Trusted Authority (RA) of the vehicle.

Dange et al. [19] suggested one cost-effective pothole detection method for detecting potholes and bumps on roads. Mobile phone sensors are used for identifying potholes and bumps. The geographical location of the potholes and bumps are acquired through the GPS sensor in mobile phone. The sensed data transmits cloud storage for carrying our future processes. This method is utilized by vehicle drivers and government authorities. The road condition is displayed in the map using android and web application.

3. PROPOSED METHODOLOGY

Some roadside unit authorizes the vehicles where the vehicles individual key was generated by RSA algorithm and token. The

road condition information was reported in ciphertext format to assure privacy against the cloud server through the random number based key generation. Third, validating the cloud server and authority of the report source, i.e., to check whether the road conditions are reported by legitimate vehicles, with the help of individual key generated by RSA. The proposed method-based road monitoring was explained here: modules System setup, sub-authority, sub-authority, Roadside unit registration, Cloud processing, RA processing. The overall process of the work is shown in Fig.1.

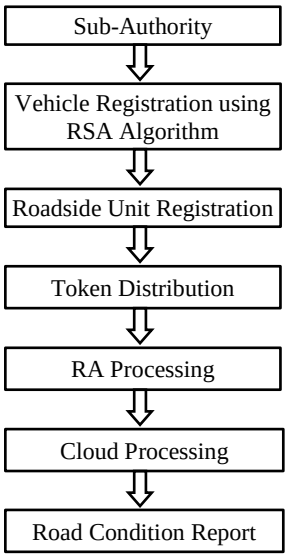

Fig.1. Proposed System

Road Authority (RA), Roadside Units (Rus), Sub-Authorities (SAs) and a cloud server are the different entities of RCoM. These are the trusted participants of VANET. The different entities of RCoM are shown in Fig.2. The authority monitors the real-time road condition with the help of a cloud server in the RA method to respond to emergency cases timely the cloud server has computing and storage resources and it provides road condition information to end-users by Cloud Service Provider (CSP). In RCoM, the vehicles gather the entire road information which RA engages.

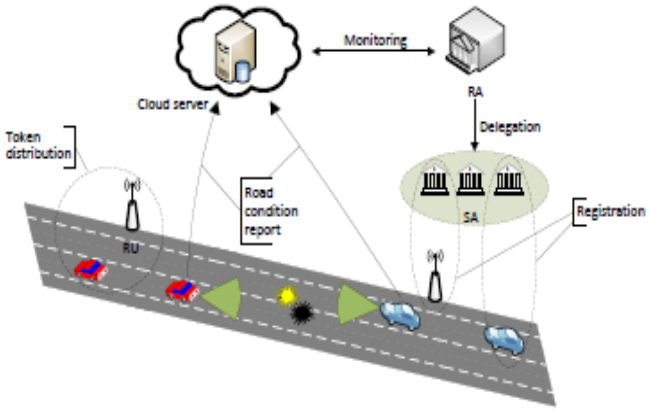

Fig.2. System Architecture of RCoM

3.1.1 Functionalities:

In designing VANET related protocol, each vehicle consists of a tamper-resistant black box containing the information and performs cryptographic operations securely. The design goals of the RCoM system are as follows.

Privacy of road condition: The cloud server does not collude with vehicles or RUs. The entire road condition information is reported in ciphertext format for privacy concern, and the ciphertext is decrypted only by the RA. The information consists of the location (roadside unit or road section). The entire report should be kept secret against the cloud server

Source authentication and token verifiability: In the RCoM system, hostile vehicles can imitate a few vehicles in reporting road conditions and fabricate a token from some RU to convince the RA to accept a fraudulent report without being detected. To prevent this attack, the cloud server verifies the source of reports without communicating with RA, and the cloud server rejects the reports if they do not satisfy the verification conditions.

Road condition classification: Many vehicles may report the same condition from the same place, and the cloud server can differentiate one information from the other in a reasonable period. The cloud server can verify whether the ciphertexts encrypt the information or not; accordingly, it groups them into equivalence classes.

3.2 SYSTEM SETUP

The RA creates a bilinear mapping $\hat{e}: G \times G! \rightarrow G_T$, in which G and G_T are cyclic groups with prime order p. The two different generators of G are g and h. Then it selects the random values x, $z \in RZ_p^*$, sets the master key $msk=(x;z)$. The x and z are represented as $w=g^z$ and $y=g^x$. The cryptographic function is given as $H_i:\{0,1\}^* \rightarrow G$. The road condition information is given as I, and the length of identities of RU is represented as λ_{ru} and λ_I. RA creates the threshold T (e.g. T=10) when T or more vehicles report the same condition at the same place, it is considered as an emergency case. The public system parameters are given as

$$\hat{e}: G;(G_T;g;h;p;y;w;H_1,H_2,\ldots,H_7,T). \quad (1)$$

3.3 SUB-AUTHORITY

The authorization of vehicle is performed using sub authorities issued by RA, and also the efficiency of the authorization process is improved. In this stage, one secret key is obtained by every SA_i from RA, such that a random value $r_i RZ_p^*$ is selected by RA for evaluating the secret key,

$$ssk_i = \left(ssk_{i,1}, ssk_{i,2}\right) = \left(g^{r_i}, h^{r_i + xH_1(SA_i)\|SSK_{i,1}}\right) \quad (2)$$

The broadcast ssk_i to SA_i securely. Sub-authority SA_i can verify ssk_i.

3.4 VEHICLE REGISTRATION

Each vehicle V_j acquires the secret keys from the corresponding sub-authority SA_i in the registration stage. The secret key vsk_j is calculated by SA_i using the RSA method.

One public key is generated and issued by RSA based on two prime numbers in accordance with an auxiliary value. In which, it is necessary to keep the prim numbers as confidential, as anyone can make use of this public key for encrypting the message. If it is prime numbers, only the authenticated and the skilled person will be able to decode the message.

RSA is a slow process, and so that it is not utilized directly for encrypting the data of the user. The encrypted shared keys are transmitted by RSA for carrying out bulk encryption-decryption processes at maximum speed in the symmetric key cryptography process [2]. Also, this RSA method is utilized for maintaining the confidentiality and authenticity of the user data.

RSA algorithm refers to an asynchronous cryptographic method utilizing pair of keys such as public and private keys. The public keys is used for decrypting the data, and the private key is used for encrypting the data. The creation of these two keys is the first step. After creating the keys, the public key is dispersed to the intermediate nodes and destination.

Step 1: Selecting two large prime numbers p and q, randomly

Step 2: Calculating $n=p*q$

Step 3: Applying Euler quotient function of n, $z=(p-1)(q-1)$

Step 4: Selecting public key e, such that it should be lesser than n, in which that e and z are prime numbers

Step 5: Selecting private key d, in such a way that if dI divided by Choose private key, d such that when d is divided by z then the remainder will be 1 i.e. ($d = e$ inverse mod z)

3.4.1 Encryption:

This process is utilized for encrypting the data which needs to be transmitted to the sink. The public key obtained from the key generation process is used by the sender so as to encrypt the data. The outputted ciphertext is sent to the destination.

Step 1: Giving the data (M) and private key (e) as inputs.

Step 2: Changing M into a number m where m is smaller than n by utilizing an agreed-upon reversible algorithm, which is named as padding technique.

Step 3: Calculating the ciphertext c as follow,

$$m=c_d \bmod n \tag{3}$$

3.4.2 Decryption:

Step 1: Providing cipher text c and public key d as inputs

Step 2: Calculating c_d

Step 3: Calculating c_d mod n

Step 4: Checking whether the result is original text m.

Step 5: At last securely transmitting vsk_j to V_j.

3.5 ROAD SIDE UNIT REGISTRATION

In the vehicle registration stage, A secret key is obtained by each road side unit RU_l from its administrative sub-authority SA_1. Here a random value r_1, $I \in RZ_p^*$ is selected by SA_1, and the secret key is calculated as,

$$rsk_1=(rsk_{l,1}, rsk_{l,2}, rsk_{l,3})$$
$$rsk_{l,1}=ssk_{l,1}, rsk_{l,2} = g^{r_1,I} \tag{4}$$

Finally, the calculated rsk_1 is securely transmitted to RU_1.

3.6 TOKEN DISTRIBUTION

If some vehicle V_j reaches a new road area, then it communicates with the administrative roadside unit RU_1. Especially, a random value $v_j \in RZ_p^*$ is selected by the vehicle and $\theta_{j,1}$ is calculated as follows,

$$\theta_{j,1} = g^{v_j}, \theta_{j,2} = vsk_{j,3} \cdot h^{v_j H_3(v_j \| RU_1 \| t_j \| \theta_{j,1})} \tag{5}$$

In which vehicle V_j transmits tuple $T_j = (SA_i, V_j, vsk_{j,1}, vsk_{j,2}, t_j, \theta_{j,1}, \theta_{j,2})$ to roadside unit RU_1, SA_I denotes the administrative authority of V_j and t_j denotes the time stamp. This step shows that some malicious vehicle cannot copy the vehicle V_j for acquiring token from RU_1. Also RU_1 fails to respond if the specified condition is not satisfied by T_j. If the given condition is satisfied, then a random value $v_1 \in RZ_p^*$ is selected by RU_1 and a token $\theta_l=(\theta_{l,1},\theta_{l,2})$ is measured. The authentication of tuple T_1 is accepted by the vehicle V_j if the condition is satisfied.

3.7 ROAD CONDITION REPORT

If Vehicle V_j collects the road information I from some portion monitored by the RU_1 in a given time, then the vehicle V_j generates one report by carrying out some functions. If a random value $2RZ_p$ is selected, then the cipher text U is evaluated as $U = (u_1, u_2, u_3, u_4)$.

At last, the ciphertext and tuple are uploaded to the cloud server by the vehicle V_j.

3.8 CLOUD PROCESSING

After the report is retrieved from the vehicle, the following steps are carried out by the cloud server.

Step 1: *Soundness Verification*: In this process, the artificial information retrieved from malicious vehicles are filtered by the cloud server. The cloud server performs one validation process for checking whether it supports the equality and also whether the report was created within a specific time period Td. If the above-mentioned conditions are met, then it is finalized that the elements received in U and V as sound; or else the retrieved elements are removed by the cloud server.

Step 2: *Privacy-Preserving Monitoring*: The cloud server combines all the sound tuples into variable equivalence classes in which the tuples in the same class report the similar road condition is similar road area in a predetermined time period.

Previously, the equivalence class was not present. The cloud server compares any one of the sound tuple (U,W) with the existing equivalence class. If (U',W′) is an element in any of the equivalence class G', then the cloud server identifies whether the specific condition is met.

If the condition is true, then the tuple (U,W) is embedded into G'; or else the cloud server differentiates it with other equivalence class. At last, new one is constructed using only one element (U, W) if there is no matching equivalence class presents.

Step 3: The cloud server transmits one element (U, W) from G to RA so as to show that an emergency condition is identified and it requests RA to give some response, if $|g| \geq T$ for the equivalence class G.

3.9 RA PROCESSING

The RA process performs the following steps: Analyzing some functions for checking the condition for performing decryption of authorized content and deciphering the ciphertext U with the master key mentioned as msk. The generated road

condition *I* is allowed at RU_1, and the necessary actions are carried out if the above-mentioned condition is met.

4. RESULTS AND DISCUSSION

Here we check the usefulness of the proposed framework IRCOM and it is distinguished with the existing methods Vehicular Cloud for Road (VCR) and RCOM method. The results were computed through delay, security rate, and throughput metrics. Through NS2 simulation environment, entire metrics were computed and implemented.

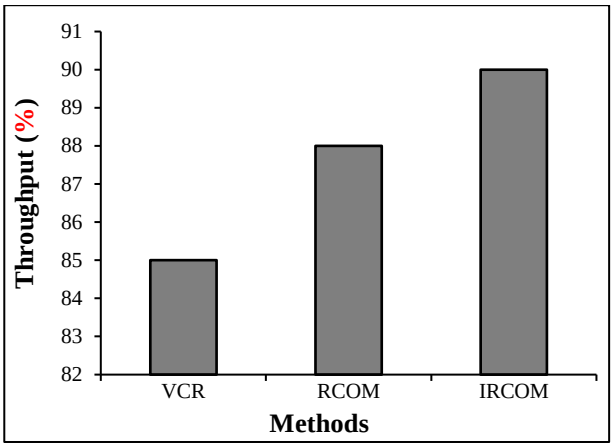

Fig.3. Throughput

In the Fig.3, Throughput results with respect to the methods like existing VCR, RCOM and proposed IRCOM model and further it shows that the newly introduced IRCOM model reduces higher throughput result which is 90% and the existing model produce 85% and 88% value correspondingly.

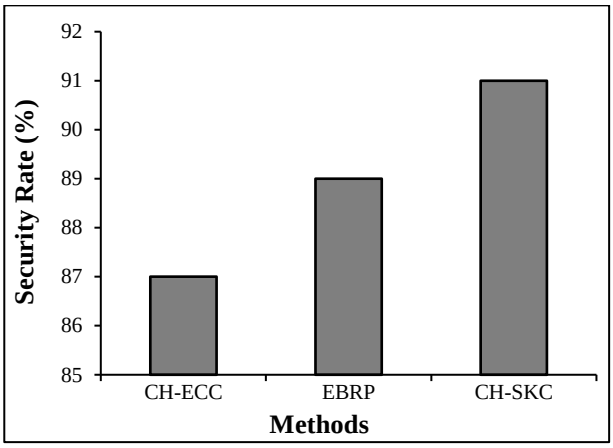

Fig.4. Security Rate

The Fig.4 explains the results of performance analysis of existing VCR, RCOM and proposed IRCOM model with respect to security rate. It shows that the newly introduced IRCOM model reduces higher security rate result, which is 91% and the existing model produce 87% and 89% value correspondingly.

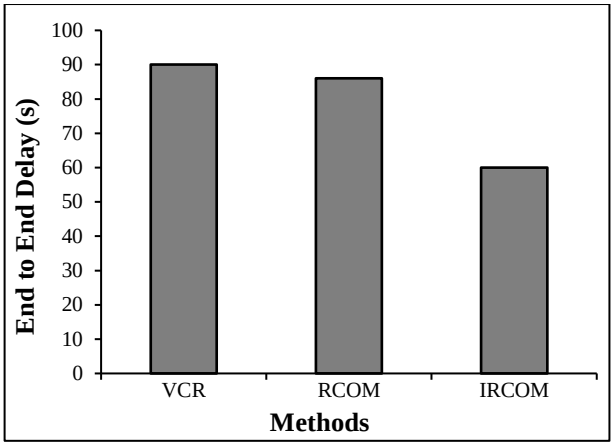

Fig.5. Delay

In the Fig.5, delay results with respect to the methods like VCR, RCOM and proposed IRCOM model is shown and further it shows that the newly introduced IRCOM model reduces lower delay result which is 60 sec and the existing model produce 90 sec and 86 sec correspondingly.

5. CONCLUSION AND FUTURE WORK

A vehicular ad-hoc network was preceded as an optimistic technique for improving the safety of the transport system and efficiency of travel. In VANET, one on-board unit is integrated into each vehicle for collecting present road/traffic condition information at a specific location and for interacting with others via distributed roadside units (RUs). Connected cloud computing (CVCC) employed for integrating VANET with cloud computing technology. By using CVCC, the cloud service provider is able to calculate and preserve the services provided. Here cloud-based road condition monitoring system (IRCOM) is designed for creating the key to register the vehicle using RSA algorithms so as to assure the secured data transmission and to avoid false information from malicious vehicles. The RU registration and the distribution of tokens are carried out by a random key generation process so as to enhance the authorization process.

Real-world trajectories and log data of vehicles are decided to utilize in future research for showing the effectiveness of this new approach. Also, the definition of events is widened, and this technique is used as a basic event-monitoring and data gathering unit for constructing a proper VANET application.

REFERENCES

[1] S. ur Rehman, M.A. Khan, T.A. Zia and L. Zheng, "Vehicular Ad-Hoc Networks (VANETs)-An Overview and Challenges", *Journal of Wireless Networking and* Communications, Vol. 3, No. 3, pp.29-38, 2013.

[2] M.B. Mansour, C. Salama, H.K. Mohamed and S.A. Hammad, "VANET Security and Privacy-An Overview", *International Journal of Network Security and Its Applications*, Vol. 10, No. 2, pp. 13-34, 2018.

[3] T.Y. Wu, Y.B. Wang and W.T. Lee, "Mixing greedy and predictive approaches to improve geographic routing for

VANET," *Wireless Communications and Mobile Computing*, Vol.12, No.4, pp.367-378, 2012.

[4] M. Umar, D. Babu and P. Singh, "Automation of Energy Conservation for Nodes in Wireless Sensor Networks", *International Journal of Future Generation Communication and Networking*, Vol. 13, No. 3, pp. 1-12, 2020.

[5] A. Daniel and K.M. Balamurugan, "A Novel Approach to Minimize Classifier Computational Overheads in Big Data using Neural Networks", *Physical Communication*, Vol. 42, pp. 1-23, 2020.

[6] J.A. Guerrero-Ibanez, S. Zeadally and J. Contreras-Castillo, "Integration Challenges of Intelligent Transportation Systems with Connected Vehicle, Cloud Computing, and Internet of Things Technologies", *IEEE Wireless Communications*, Vol. 22, No. 6, pp.122-128, 2015.

[7] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin and H. Wang, "Privacy-Preserving Cloud-based Road Condition Monitoring with Source Authentication in Vanets", *IEEE Transactions on Information Forensics and Security*, Vol. 14, No .7, pp. 1779-1790, 2018.

[8] B. Al-Otaibi, N. Al-Nabhan and Y. Tian, "Privacy-Preserving Vehicular Rogue Node Detection Scheme for Fog Computing", *Sensors*, Vol. 19, No. 4, pp. 965-982, 2019.

[9] Y. Agarwal, K. Jain and O. Karabasoglu, "Smart Vehicle Monitoring and Assistance using Cloud Computing in Vehicular Ad Hoc Networks", *International Journal of Transportation Science and Technology*, Vol. 7, No. 1, pp. 60-73, 2018.

[10] H. Tan, D. Choi, P. Kim, S. Pan and I. Chung, "Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs", *Wireless Communications and Mobile Computing*, Vol. 9, No. 2, pp. 1-14, 2018.

[11] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer and B. Qin, "Privacy-Preserving Vehicular Communication Authentication with Hierarchical Aggregation and Fast Response", *IEEE Transactions on Computers*, Vol. 65, No. 8, pp. 2562-2574, 2015.

[12] M.S. Sheikh and J. Liang, "A Comprehensive Survey on VANET Security Services in Traffic Management System", *Wireless Communications and Mobile Computing*, Vol. 12, No. 1, pp. 1-24, 2019.

[13] L. Zhang, D. Gao, C.H. Foh, D. Yang and S. Gao, "A Survey of Abnormal Traffic Information Detection and Transmission Mechanisms in VSNs", *International Journal of Distributed Sensor Networks*, Vol. 10, No. 5, pp. 1-13, 2014.

[14] S.C. Radopoulou and I. Brilakis, "Improving Road Asset Condition Monitoring", *Transportation Research Procedia*, Vol. 23, No. 1, pp. 3004-3012, 2016.

[15] L. Forslof and H. Jones, "Roadroid: Continuous Road Condition Monitoring with Smart Phones", *Journal of Civil Engineering and Architecture*, Vol. 9, No. 4, pp. 485-496, 2015.

[16] S. Sattar, S. Li and M. Chapman, "Road Surface Monitoring using Smartphone sensors: A Review", *Sensors*, Vol. 18, No. 11, pp. 1-21, 2018.

[17] L. Zhang, X. Men, K.K.R. Choo, Y. Zhang and F. Dai, "Privacy-Preserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud", *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 3, pp. 1-14, 2018.

[18] L. Liu, Y. Wang, J. Zhang and Q. Yang, "A Secure and Efficient Group Key Agreement Scheme for VANET", *Sensors*, Vol. 19, No. 3, pp. 482-494, 2019.

[19] M.T. Dange, D. Pawar, R. Potdar, S. Kaul and P. Pawar, "Evaluation of Road Condition using Android Sensors and Cloud Computing", *Evaluation*, Vol. 6, No. 2, pp. 1120-1124, 2019.