Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Volume II, Issue II

FAST Data Dissemination MODEL in VANETs Using FOG

Kapil Sharma[1] and Deepak Motwani[2]
[1]*Department of Computer Science, Amity University Madhya Pradesh, Maharajpura Dang, Gwalior (MP) 474005, ksharma@gwa.amity.edu*
[2]*Department of Computer Science, Amity University Madhya Pradesh, Maharajpura Dang, Gwalior (MP) 474005, dmotwani20005@gmail.com*

***Abstract*-In today's modern era we need to develop intelligent transportation system. There should be system that is both secure and also reliable. We want to create a frame work in which the vehicle can send its information from one vehicle to another in the shortest possible time. For the solution of this problem, we start working on FAST Data Dissemination MODEL for VANETs using FOG Phase-I.**

***Keywords*- VANETs, RSU, DSRC, OBU, cloud, TOEFVC, TOEFV, FOG.**

I. INTRODUCTION

VANET means vehicular Ad-Hoc network. VANET is the group of Smart Vehicle it consist various component i.e. Road Side UNIT (RSU), On Board Unit (OBU) and Trusted Authority.

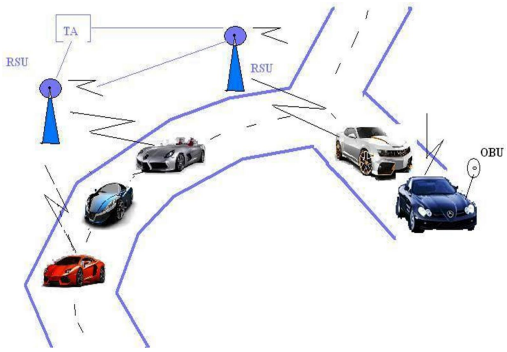

Figure 1: VANET Architecture

VANETs Architecture is a group of intelligent transport systems. In this system we can send messages from one vehicle to another, as shown in figure 1.
As shown in this diagram, we can send a message to a group of vehicles and also check that message. After checking, we can find out whether the correctness of the message is correct or not. The most important point in intelligent transport system is how quickly the message can reach the receiver. For this, many research scholars have written research papers, how to get the message from one car to another in a fixed time so that we can reduce the death rate due to accident due to traffic.

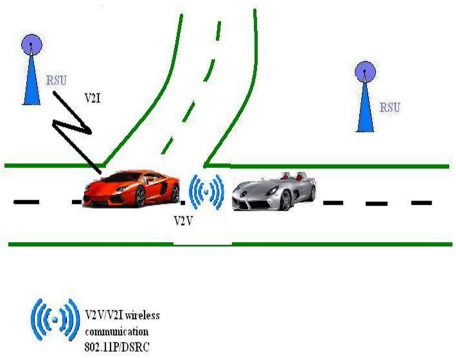

Figure 2: Types of Communication

The figure 2 shown above shows the communication used in VANETs. VANETs mainly consists of three types of communication such as vehicle to vehicle communication, vehicle to infrastructure communication and infrastructure two vehicle communications. The DSRC protocol is used for communication in the VANETs architecture. DSRC means dedicated short-range protocol, how many types of messages are within this protocol and what should be their range and what should be their class, given inside the protocol. In DSRC, we mainly see two types of messages, the first is a critical message and the second is a non-critical message. Critical messages work on real time. We have to send information as quickly as possible, like when there is an accident and there is a terrorist attack, atthat time, we use a critical type of message. And when we have to send location, petrol pump, restaurant information, and then we have to use non-critical type messages.

II. RELATED WORK

Data is exchanged between vehicles by VANETs. This type of transmission in VANETs is full of many choices. Network metrics in VANETs change continuously due to the high node mobility, dynamic topology in VANETs. There is a protocol used in this research paper called DDRX. The results of this paper show that the number of

packets transmitted by DDRX, delay and packet loss gives information about efficiency data [1].
Author in this research paper has worked on the proposed approach called SIVNFC. This model works simultaneously at the node level and network level security. In addition to security, fog computing has also been used. The SIVNFC model works to prevent DoS attacks across the network [2].
This research paper using Algorithm is designed to work on data collection and real-time data using fog computing. The simulation results of this paper show that this method works well on reliability, data accuracy. This method can prevent data abnormalities in the right way and can also increase security [3].
In this paper work has been done on fog computing and trust. In this paper, using Fog computing, a solution has been given on how to establish trust between two vehicles from the Internet of Vehicles (IoV) and the Social Internet of Vehicles (SIoV) [4].
In this research paper, researchers have worked on the data dissemination model. For example, there are similar traffic directions, uneven directions and multi-directions. The data we get from each vehicle. Work has been done on the reasons of how to store it and spread it safely [5].
In this research paper, researchers have worked on various trust models and how to make trust stable in VANETs. What are the attachments in this environment which threatens the network and what is the truth of the message that is sent, it is all told in this paper [6].
In this paper, work has been done on decentralized and scalable privacy-preserving hybrid cryptography. Plans have been prepared for secure communication in VANETs. In this paper, the communication network is divided into several domains areas that are monitored locally by ATAS [7].
Research has been done on WSN and cloud computing in this paper. We have seen in this paper that using sensors, work has been done in different areas. Such as industry, agriculture, transportation, medical, military etc. And in this paper work on trust computation has also been done [8].
In this research paper, work has been done on trust computation. In this paper we have compiled trust mainly using the Theory of Evidence and classified the trust level using the fuzzy analyser in its result. After that in this paper, we have applied the reward penalty algorithm. Through this algorithm, the trust value of the node that makes a mistake through this algorithm is reduced. And the information of the node is correct and which does not misbehave. The trust level of that node is increased [9].
In the previous paper we saw how trust is computed. In this paper, we have seen how the data will arrive on time. In this paper, cloud computing has been used. By using the cloud, we have achieved success in reaching a certain amount of time for data dissemination. But the demand of the present time is that the transmission of data should be fast. We need a technique to solve this problem [10].
In this paper, researchers have talked about the security challenges of Fog and Cloud [11].

III. PROBLEM FORMULATION

We reviewed the deep literature and found that sending messages on time is very important. If the message does not arrive on time, then the message has no value. That message is unusable, we have seen in previous papers that researchers have worked on many algorithms and frameworks. So that the data can be accessed on time, out of these research papers, I also have a research paper in which we applied TOEFV model. We computed trust and used cloud computing for fast data transmission. But now we want the message to reach the receiver at a faster speed, for this, we have to create some framework that can deliver the message to the receiver within our time. So that we can review the scheduled time and take action on it.

IV. PROPOSED WORK

In this research paper, we have succeeded in knowing from literature that if we work on intermediate layer, we can do fast data transmission. Under this, we have proposed a solution. That if we create a frame work in which we are intermediate layer then we can do fast data transmission. For this we are preparing a model using the fog layer. This model will solve our problem. What will be the algorithm of this model; we will expand it in the next research paper Phase-II.

V. CONCLUSION AND FUTURE WORK

In this research paper, we learned that if an intermediate layer is placed between the cloud and the infrastructure, the transmission of data can be fast. Like if we talk about the client server system, when the client sends a request to the server for the first time, then it takes some processing time from the server to the client. If the client stores the response of the server in an intermediate layer such as cache memory and the client sends the same request again, the response gets from the cache memory and the time to reach the server is saved. We have made this example as part of our future research. We can also access the data faster by using the fog layer between cloud and infrastructure in the future. We will expand how these layers work in the next research paper.

REFERENCES

[1] Joahannes B.D.daCosta, Allan M. de Souza, Denis R., EduardoCerqueira, and LeandroA.Villas, "Efficient data dissemination protocol based on complex networks metrics for urban vehicular networks", *Journal of Internet Services and Applications, Springer open access,* pp.1-13,2019.

[2] Samuel Kofi Erskine and Khaled M. Eileithyia,"Secure Intelligent Vehicular Network Using Fog Computing", *Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT 06604, USA, MDPI, electronics,* pp.1-25,2019.

[3] Guangwei Zhang and RuifanLi, "Fog Computing Architecture-Based Data Acquisition for WSN Applications", *services and communications in fog computing, china communications*, pp. 69-81, 2017.

[4] RaziIqbal, Talal Ashraf Butt, Muhammad Afzaal and Khaled Salah, "Trust management in social Internet of vehicles: Factors, challenges, block chain, and fog solutions", *International Journal of Distributed, Sensor Networks*, pp.1-22, 2019.

[5] Tamer Nadeem, Pravin Shankar and LiviuIftode, "A Comparative Study of Data Dissemination Models for VANETs" *IEEE*, pp. 1-10, 2006.

[6] Seyed Ahmad Soleymani, Abdul Hanan Abdullah, et.al., "A Secure Trust Model based on Fuzzy Logic in Vehicular Ad Hoc Networks with Fog Computing", *IEEE*, pp. 2169-3536 ,2017.

[7] Shrikant T, Sunilkumar S. M., and Pascal L. "Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, pp.1-10, 2018.

[8] Gangue Zhang, Tian Wang, Guojun Wang, Anfeng Liu WeijiaJia, "Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system", Concurrency Computer at Pract Exper John Wiley & Sons, Ltd, pp.1-13, 2018.

[9] Kapil Sharma, Brijesh Kumar Chaurasia, Shekhar Verma and Arpita Bhargava, "Trust computation in VANET using TOEFV", International Journal of Trust Management in Computing and Communications, pp.36-51, 2017.

[10] Brijesh Kumar Chaurasia and Kapil Sharma, "Trust Computation in VANET Cloud", Transactions on Computational Science XXXIV, Springer, pp.77-95, 2019.

[11] Vipul Tiwari and Brijesh Kumar Chaurasia, "Security Issues in Fog Computing using Vehicular Cloud", *IEEE conference,* pp.1-4, 2017.