CGC International Journal of Contemporary Technology & Research
ISSN: 2582-0486 (online), Vol.-2, Issue -1 DOI: 10.46860/cgcijctr.2019.12.20.57

Safety Message Dissemination in Cloud-VANET based Infrastructure through Game Theory

[1]Deepika Verma, [2]Parminder Singh
[1,2]Department of Information Technology, CEC,Landran
[1]deepika.verma1407@gmail.com, [2]singh.parminder06@gmail.com

Abstract: **Vehicle ad hoc networks are usually equipped with electronic chips that store a lot of sensitive information. Stores information related to routing tables, packet, packet header information, uplink and downlink speed. Many studies emphasize on transmission delays, data redundancy, queue delays and buffer management. The existing scenario collects results while transmitting packets from the source machine to the destination machine. In the enhanced view, collect results from a remote server located in a rural area. Data was collected through a cloud-based infrastructure. In this paper, we propose a framework for message propagation and provide security to end to end semantic. The benefit of this framework is to provide correct information to the end user through cloud technology. This hybrid model is capable of facilitating communication for cellular based infrastructure. To evaluate the proposed model, we collect the results from the NS-2 simulator.**

Keywords: **Cloud Computing, Vehicular Ad hoc network (VANET), Packet Header.**

I. INTRODUCTION

Nowadays, VANET Technology is not limited to the transmission of information to vehicles. It is also cooperating with other technology based infrastructure. It promotes hybrid technology design and is beneficial to society. Generally, when a hybrid technology is used by society, it also produces a negative effect which is bad for the better society. In this paper, we address issues of VANET-Cloud Communication and also provide security to the hybrid model when transferring and receiving information. Use of the Vehicle Cyber Physical System (VCPS) [1], accurate transmission of information, route suggestions and accident alerts. Vehicle systems can be attacked by disrupting peer network routes or by incorrect or corrupting the information contained in the routing protocol. Generally, the hacker modifies the information contained by the routing protocol. Spoofing routing information usually causes systems to misbehave with each other, cause a Denial of Service (DOS) attack, or cause traffic to follow a route that is not normally performed. There are several consequences of malfunctioning of routing information:

1. It is also a hacker's job to redirect traffic to create routing loops
2. Redirecting traffic and therefore can be monitored over an insecure link
3. Redirecting traffic to cancel it

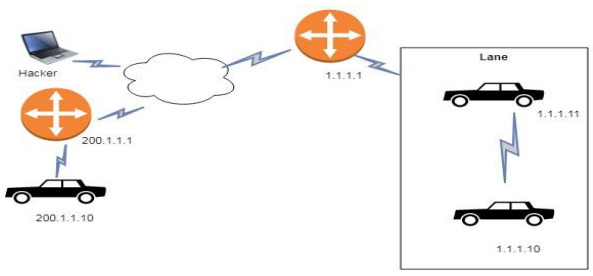

Fig. 1. Security Attack in VANET

As illustrated in figure 1, vehicle A (1.1.1.10) transmit the data to vehicle C (200.1.1.10) through gateway G1 (1.1.1.1) and G2 (200.1.1.1). Let us consider, the attacker has been connected directly to gateway G1 and G2 and send the false routing information to G1 indicating that G2 is the preferred destination to the network 200.1.1.0/24. However, G1 has a routing table entry to the 200.1.1.0/24 network, the new routing entry stored in the routing table. Consequently, when vehicle A connect to vehicle C for packet transmission then the packet received from G1 to G2 through cloud technology. G2 received the packet and does not forward the packet vehicle C. instead, it routes the packet to G1 because the apparent best route to 200.1.1.0/24 is through G1. Packet received by G1, it looks in its routing table and find legitimate route to the G2 and forward back to G2, creating the loop. The loop was caused by misinformation injected into the Gateway G1. The problem can be partly solved of the RFC 4593, Generic Threats to routing protocol. In [1], the author put forward safety message in VANET, in which the vehicles collide together and the accidental information are not disseminated properly due to inclement weather condition. As a result, information was congested and not reported to the cellular network.

Despite the importance of current solutions, we note that smart vehicles are connected to more devices and networks. Unfortunately, there are more attacks on the attack surface to the attacker [2]. An attack surface is the total sum of vulnerability in the given network that is accessible to an attacker. As we have already seen in Figure 1, an attacker modifies the routing table and controls the entire traffic. The attack surface contains open ports in data centers, hosts, connected devices; Software based systems, wireless equipment or connected vehicles. Attacks on the internet are constantly increasing due to the Internet of Things (IoT) and 5G networks. Other connected devices, generating a lot of IP based traffic, increase the likelihood of a network attack.

The cloud computing paradigm discussed in many literatures, Cloud-VANET performance can be classified in terms of performance point of view are speed based lane changing, collision avoidance, video surveillance, vehicle accident detection and broadcast emergency messages have elaborated by the authors [3]. All the moving vehicles on the road have been monitored through onboard unit which is installed in the vehicle. The onboard unit (OBU) is passing authenticate information to the peer, emergency vehicle treats on priority basis. All the disseminated messages stored in the

roadside units and passed to the central server supported by cloud architecture. Onboard unit perform the operations like speed detection, vehicle detection, location of the particular vehicle, information related to messages and automatic break signal. The interface of OBU connected to mobile application for further analyzing of data.

Generally speaking, cloud-IoT based model require more attention during delivery of data [4]. Delivered data has been captured by anonymous user and create problem for the organization. Mobile devices that are connected to the cloud-based infrastructure cannot be physically controlled on the premises of an organization. They can be lost, tampered, spoof with, putting data and network access at risk. Game Theory (GT) approach brings attention related to these issues and prevents the cyber security attacks. Attacks can be identifying through stackelberg security games (SSG) and machine learning technique which helps to make effective decision on cyber warfare. It was proven by the approach to tackle such denial of service type attacks and predict future behavior of nodes.

VANET aggregation in intelligent transportation systems, refers to information and communication technology (applied to transport infrastructure and vehicles) that improves transport outcomes such as transport safety, transport productivity, travel reliability, informed travel choice. Interest in ITScomes from the problems caused by traffic congestion and an alliance of new information technology for simulation, real-time control, and communications networks. Congestion reduces efficiency of transportation infrastructure and increases travel time, air pollution, and fuel consumption [7]. The main components in this system are: Application Unit (AU), On Board Unit (OBU) and Road Side Unit (RSU). To process the information, OBU and set of sensors are connected to the vehicles. Wireless medium used to dissemination the information to other vehicles or RSU. The Vehicular Ad-Hoc Network Architecture is depicted below in Figure 2.

RSU joins an application that provides services, and OBU uses these services. RSU provides the services to AU's to connect various vehicles to the Internet. The dissemination of RSUs and total number of RSUs are subject to the VANET protocol, which is to be used. Although it is safe to assume that infrastructure exists to some extent and vehicles have access to it erratically, it is unrealistic to require that vehicles always have wireless access to roadside units [5].

II. Literature Survey

The Authors [6]had analyzed that rather than using the static algorithms for shortest path a bio inspired system Ant-based vehicle congestion avoidance system (AVCAS). To find out the least congested shortest path this system uses the average travel speed prediction. This also helped to reduce traffic congestion with map segmentation and average travel speed prediction. To overcome the dynamicity and quick changes of vehicular environment segmentation and short-term predication had been used.

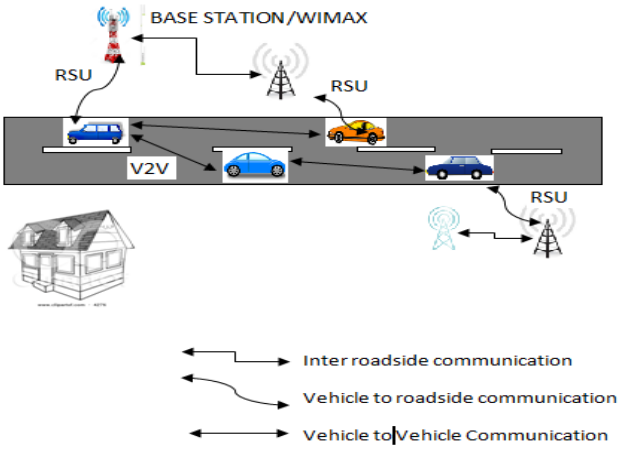

Fig 2. VANET Architecture

The Authors [7] had discussed E-ACO-DSR a routing algorithm that inspired from biological system to handle emergence and self-organization. Concluded that E-ACO-DSR could produce low routing overhead, minimum end-to-end delay, broken route, energy consumption and high packet delivery ratio. Authors had analyzed that E-ACO-DSR was efficient to performed congestion avoidance, significant energy consumption and link breakage. All ACO based algorithms ACO-DSR, AD-ZR, hybrid genetic and particulate swarm intelligence based algorithm HGAPSO, genetic based algorithm EMRGA and original DSR had been compared to E-ACO-DSR in both cases spars and dense MANET.

In this paper authors [8] had introduced an ant colony optimization based algorithm Time-Ants, which resolved favorable trail for vehicular traffic in both space and time dimensions by assigned the pheromone value to each road. Author had described the different types of swarm intelligence based algorithm like bee-based algorithm, ant based algorithm, firefly based algorithm, particle swarm based algorithm.

The paper evaluated the most popular routing protocols Ad-hoc On Demand Routing protocol (AODV), Distance Vector Routing Protocol (DSR), are reactive routing protocols, and On demand Link state Routing Protocol (OLSR) proactive routing protocol for MANET and VANET. Authors [9] observed that the performance of these routing protocols had evaluated only for the general traffic case but in this paper authors had tested the performance of these algorithm for multimedia traffic and especially video transmission.

The authors [10] had analyzed that there was no need to join a BSS if stations operating WAVE mode. Stations could exchange data by utilizing the BSSID that was available at all time. The connection setup overhead and safety application have been reduced self-acting for vehicles. DSRC provides the better services than the private services. The mechanism defined for WAVE BSS start the process from initiating station only receiving a single WAVE Advertisement Message. With the help of Wildcard BSSID, WAVE BSS had been to send and receive data further. Authors analyzed that, the different layers of all the protocols had been related in the DSRC standards and communication stack.

Table I: Brief Description of important Articles

Paper	Detailed Description	Disadvantages
[1]	VANET based system suffers from issuesrelated to throughput and latency. This means when the infrastructure deployed in heterogeneity environment over cloud based infrastructure then it is quite impossible to disseminate the messages. In addition, the suggested framework uses data downlink dissemination strategy to combat problems encountered in VANET-Cloud infrastructure.	The mathematical analysis of the suggested model is made by the authors.
[2]	The proposed model suggested by the authors investigated the potential of the VANET. This article investigates the various attacks that are coming through the Controlled Area Network Bus (CAN), the Electronic Control Unit (ECU) and the inter-vehicle communication. Finally, a possible solution to isolate these attacks that are coming from different locations can be resolved through cryptography methods and intrusion detection systems.	The suggested model is a review based system and the suggested techniques overload the entire system which affects the performance of the system.
[3]	The paper discussed the issues in VANETs model are speed based lane changing, collision avoidance and time of arrival based localization. The proposed model intelligently controls the traffic of vehicles which is connected to the cloud model. This result manages the speed based lane changing and avoid the collision in between roads.	The limitation of this model is lack of security, resultant any malicious node attack the network system. Another issue, due to high consumption data offloading may increase the energy which decline the performance of the VANETs system.
[11]	The number of broadcast schemes is suggested in the VANET based models; security messages and their reliability issues are being explored further. in this article, reliable and timely security messages are supplied to enhance the quality of the VANET model. The proposed model also highlights the collision model that can be used in the wave / 802.11p standard.	Authors examine performance in common networks; They could not split multi-hop based views into the article. In addition, VANETs performs in hop-based scenes in real-time network.
[12]	Internet of Vehicles (IoV) provides information transfer to other vehicles through the multi-hop concept. Usually connected vehicles pass messages to other vehicles by hop alone, which is very difficult to reach in rural areas. In fact, the authors investigate congestion traffic that can be avoided through clustering. This model also provides protection during message communication, calculating the value of the hash at the start of messages from source vehicle.	The waiting period quickly increases during the route diversion decision.
[13]	The authors have compared two ADHoc models in the wireless viewpoint with the vehicle ad hoc network and the mobile ad hoc network, but the vehicle ad hoc network is needed today. The study focuses on the challenges of communication and operation in the three possibilities for vehicle to vehicle, vehicle to infrastructure and hybrid architecture. The protocol stack for the network of vehicles deals with the communication between the nearest vehicles.	The authors surveyed different technologies and technologies associated with vehicle-ad-hoc networks .There are still many security issues that need to be addressed in vehicle communication.
[14]	The authors have worked on the smart transport system in which they provide the effective solution for road accidents. inspite of effective communication they provide the security in messaging services. for communication perspective, mobile control transport system protocol has been used to handle web based applications.	The proposed model effective in IEEE 802.11p model but it cannot extend up to IoT based technology.

III. Proposed Model

The proposed work mainly deals with the cyber security attacks and transfer maximum time of data dissemination among the vehicles and vehicles in roadside units. The cloud-VANET based model comparing the previous work and the proposed work does evaluation. The previous scenario consists of simple cyber security attacks that only access the information but fail to isolate the attacks, which leads to the more time delay and more throughput with high packet delivery. The proposed work flowchart adds the new features in to previous work. Various feature that has been added in the framework.

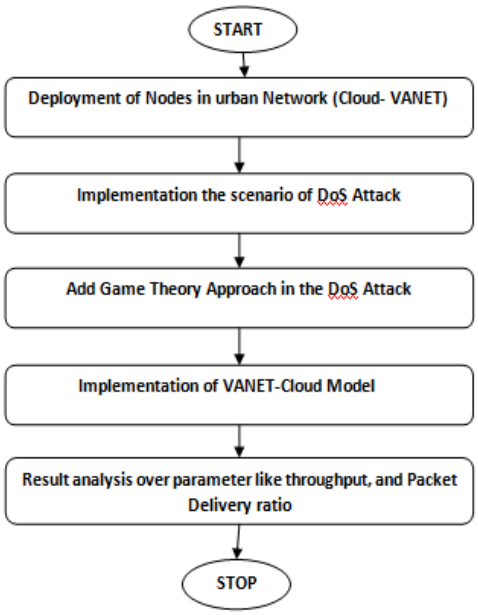

Fig. 3. Proposed Cyber Security Model for Cloud-VANET Architecture

Proposed Model of Game Theory

```
for k = 1 to m  do              //k initialize as vehicles
 for i = 1 to n do              // I initialize as roads
 ant[k].visited[i] ← false
 end-for
 end-for
 step ← 1
for k = 1 to m do
 r ← random{1, . . . , n}
 ant[k].tour [step] ← r
ant[k].visited[r ] ← true
 end-for
 while (step < n) do
 step ← step + 1
 for k = 1 to m do
Neighbor List As Decision Rule (k,step)
 end-for
 end-while
 for k = 1 to m do
 ant[k].tour [n + 1 ] ← ant[k].tour [1 ]
 ant[k].tour length ← ComputeTourLength(k)
end-for
 end-procedure
```

IV. Experimental Setup

The simulation is carried out using the Network simulator (version 2.35), which simulates the events such as sending, receiving, dropping, forwarding, etc. The wireless channel is used as the vehicular nodes deployed communicate wirelessly with each other. The propagation models are used to compute the received power. They follow the pattern of distinct signal criteria in which the vehicle moves only when the signal received. The two-Ray ground Radio propagation model is used. An omni-directional antenna is employed for carrying out the transmissions, which can transmit signal over a 360-degree angle. Omni-directional wireless sensor networks are modeled such that a bidirectional link is established between neighboring sensor nodes if they are within communication radius. A grid structure scenario with 26 nodes, 15 traffic lights and one base station have been deployed in 1200*1200 m^2 area as shown in fig 4 below. Vehicles are represented in green color; traffic lights in red color initially and base station in blue color. Traffic lights in the simulation work as real traffic lights system. The following table gives an overview of all the simulation parameters used.

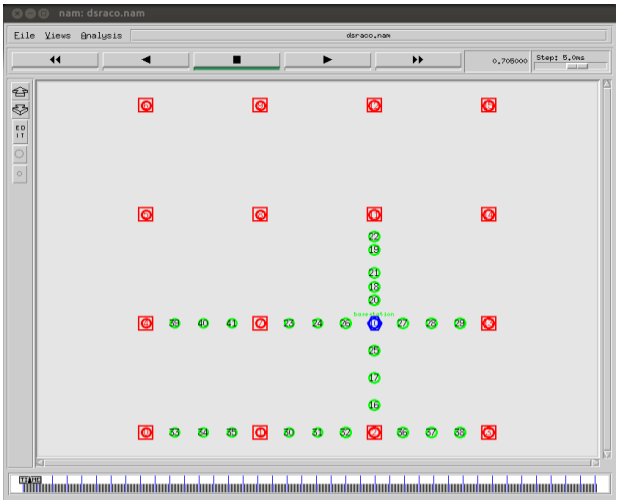

Fig. 4. Experimental Setup for Cloud-VANET Scenario

The parameters that are configured in scenario are described given below:

Table II. Simulation parameter configured in scenario

PARAMETERS	VALUES
Simulator	NS-2.35
Channel Type	Wireless Channel
Mobility Model	Two-Ray ground Radio Propagation Model
Network Interface Type	Wireless Phy/IEEE 802.11
Antenna Model	Omni-directional
Number of vehicular-nodes	26
Routing Protocol	DSR
Simulation Time	40 sec
Network Size(m*m)	1000 *1000
TCP- Variants	TCP-New Reno
Network	Cloud

V. Performance Evaluation

Throughput: is amount of data transferred from one place to another or processed in a specified amount of time. According to proposed work throughput is the average rate of successful message or packet delivered over a communication channel. Throughput is measured in terms of bits/sec or bytes/sec.

Table III. Throughput Comparison

Throughput (Mbps)	Previous Work	Proposed Work
Minimum value	14	15
Average value	39	41
Maximum value	92	94

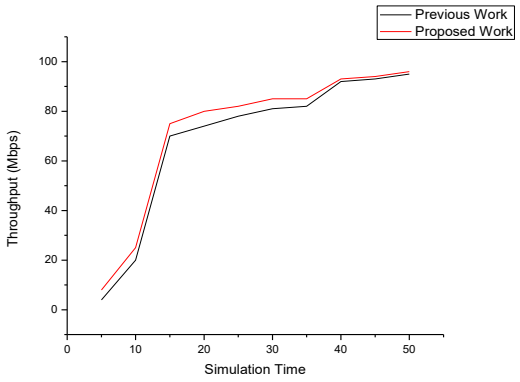

Figure 5. Throughput Comparisonwith and without proposed work

Packet Delivery Ratio: Packet Delivery Ratio is ratio of number of successfully received data packet by the destination as compared to the number of data packets sent by the sender. As the value of packet delivery ratio increases it refer better performance of protocol. In VANETs Packet delivery ratio is measured in terms of total packets send over the total packets received per second.

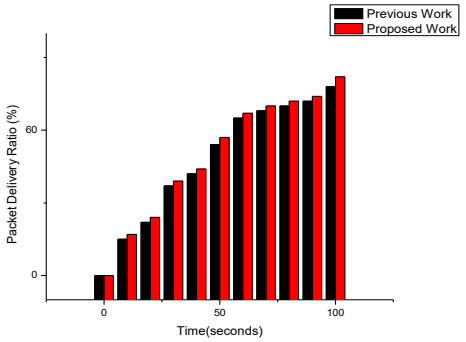

Figure 6: Packet Delivery Ratio comparison graph with and without proposed work

Table IV. Packet Delivery Ratio (%) Comparison

PDR (%)	Previous Work	Proposed Work
Minimum value	15	17
Average value	42	44
Maximum value	78	82

VI. CONCLUSION

The purpose of VANETs is to provide communication networks to transfer information regarding traffic, roads side units, and other vehicles cost efficiently and fast. These networks act as traffic and route guide to assist passengers. These networks have been practically realized in many countries like JAPAN, owing to these features. Efficient and scalable information transfer to V2V and V2I is challenging due to dynamic behavior of VANETs, which leads to congestion. The simulation result of proposed algorithm yielded the better performance than simple DSR algorithm. For the future scope, this work can extend to large network with more number of vehicles and roadside units. Future work might be focus on to use geographic routing protocol. Wi-MAX scalability issues of network can be resolving in future work.

REFERENCES

[1]. B. Liu, D. Jia, J. Wang, K. Lu, S. Member, and L. Wu, "Cloud-Assisted Safety Message Dissemination in VANET – Cellular Heterogeneous Wireless Network," vol. 11, no. 1, pp. 128–139, 2017.

[2]. X. Li, Y. Yu, G. Sun, and K. Chen, "SECURITY AND PRIVACY OF CONNECTED VEHICULAR CLOUD Connected Vehicles ' Security from the Perspective of the In-Vehicle Network," no. June, pp. 58–63, 2018.

[3]. Y. Agarwal, K. Jain, and O. Karabasoglu, "International Journal of Transportation Smart vehicle monitoring and assistance using cloud computing in vehicular Ad Hoc networks," *Int. J. Transp. Sci. Technol.*, vol. 7, no. 1, pp. 60–73, 2018.

[4]. V. Damjanovic-behrendt, "Stackelberg Security Game for Optimizing Security of Federated Internet of Things Platform Instances," vol. 11, no. 5, pp. 529–534, 2017.

[5]. S. F. Tzeng, S. J. Horng, T. Li, X. Wang, P. H. Huang, and M. K. Khan, "Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, 2017.

[6]. M. Reza, A. Jalooli, E. Shaghaghi, L. Rothkrantz, R. Hafeez, and N. Badrul, "Engineering Applications of Arti fi cial Intelligence Ant-based vehicle congestion avoidance system using vehicular networks," vol. 36, pp. 303–319, 2014.

[7]. S. Chatterjee and S. Das, "Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network," *Inf. Sci. (Ny).*, vol. 295, pp. 67–90, 2015.

[8]. S. Roy, "Nature-Inspired Swarm Intelligence and Its Applications," *IJECS-MECS*, no. December, pp. 55–65, 2014.

[9]. Z. Qian and Z. Ya-Qin, "Cross-Layer Design for QoS Support in Multihop Wireless Networks," *Proc. IEEE*, vol. 96, no. 1, pp. 64–76, 2008.

[10]. Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-Vehicle Safety Messaging in DSRC," pp. 19–28.

[11]. S. Sattar, H. K. Qureshi, M. Saleem, S. Mumtaz, and J. Rodriguez, "Reliability and energy-efficiency analysis of safety message broadcast in VANETs," *Comput. Commun.*, vol. 119, no. June 2017, pp. 118–126, 2018.

[12]. D. B. Rawat, M. Garuba, L. Chen, and Q. Yang, "On the security of information dissemination in the Internet-of-Vehicles," *Tsinghua Sci. Technol.*, vol. 22, no. 4, pp. 437–445, 2017.

[13]. F. Cunha *et al.*, "Data communication in VANETs: Protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90–103, 2016.

[14]. D. Verma and P. Singh, "Efficient Authentication and Privacy Mechanism to protect legitimate Vehicles in IEEE 802.11p Standard," *Int. J. Mod. Educ. Comput. Sci.*, vol. 11, no. 1, pp. 39–44, 2019.

[15]. https://www.ietf.org/rfc/rfc4593.txt